JINSHIDAISHUJICHU

近世代数基础

牛凤文 编

吉林大学
出版社

JINSHI
DAISHU
JICHU



ISBN 7-5601-2729-0/O·278
定价:9.50元

近世代数基础

牛凤文　编

吉林大学出版社

图书在版编目（CIP）数据

近世代数基础/牛凤文编. —长春：吉林大学出版
2002.8
ISBN-7-5601-2729-0

Ⅰ.近... Ⅱ.牛... Ⅲ.抽象代数—高等学校—教材 Ⅳ.O153

中国版本图书馆 CIP 数据核字（2002）第 050494 号

近世代数基础

牛凤文 编

责任编辑、责任校对:赵洪波　　封面设计:孙　群

吉林大学出版社出版　　吉林大学出版社发行
（长春市解放大路 125 号）　　长春市永昌福利印刷厂印刷

开本:850×1168 毫米　1/32　　2002 年 8 月第 1 版
印张:6.25　　2002 年 8 月第 1 次印刷
字数:146 千字　　印数:1—1 000 册

ISBN 7—5601—2729—0/O·278　　定价:9.50 元

前　言

近世代数课是数学专业本科生的基础课，讲述基本代数体系的结构．本书分别介绍群、环、模的结构理论．群的理论在历史上出现得最早，研究内容最丰富，研究方法最具典型性，同时也是代数学中应用最广泛的分支，本书略深入地讨论了群论的几个重要课题．

抽象代数的思想方法正向各个科学领域渗透并不断产生新的分支，本书不追求知识的完整性而力求把有关商、同态、扩张等重要的思想方法的内涵讲透．

定理和命题的选择不只注重其本身在理论体系中的重要性，也考虑到它的证明方法的示范性．

本书是在笔者多年于吉林大学讲授近世代数课所用的各种讲义的基础上，吸收自己的老师、同事们的教学改革成果，逐步修改完成的．

一般情况，在60个学时内可顺利完成全部教学内容．如果时间不充裕，第三章§5和第七章§3的内容可酌情删减，而不影响整体连贯性．

作者真诚地期待同行和读者提出宝贵意见．

牛凤文

2002年4月

目　　录

记　号

本书用大写英文字母 $A, B, C, \cdots$ 代表集合，用小写英文字母 $a, b, c, \cdots$ 代表元素.

$a \in A$ 表示 a 是集合 A 的一个元素，也说 A 含 a 或 a 属于 A，a 在 A 中.

$a \notin A$ 表示 a 不是集合 A 的元素，a 不在 A 中，也说 a 不属于 A，A 不含 a.

$A \subseteq B$ 表示集合 A 是 B 的子集，A 的每个元素都是 B 的元素.

$A \subseteq B$ 但 $A \neq B$，则说 A 是 B 的真子集.

用 $\varnothing$ 代表空集，空集是任意集合的子集.

用 $\mathbf{N}^*$，$\mathbf{N}$，$\mathbf{Z}$，$\mathbf{Q}$，$\mathbf{R}$，$\mathbf{C}$ 分别代表正整数集、非负整数集（自然数集）、整数集、有理数集、实数集和复数集.

集合 A 的所有子集组成的集合称为 A 的**幂集合**. 集合 A 的若干子集组成的集合称为 A 的一个**子集族**. 有时把 A 隐去简称为集族.

设 A 是一个集合，I 是个集合，I 的每个元素 i 对应 A 的一个子集 A_i，则说集族

$$\{A_i \mid i \in I\} \tag{1}$$

是用 I 标号的，I 是该集族的**标号集**.

集族(1)中所有集合的交集记为 $\bigcap_{i\in I} A_i$，即

$$\bigcap_{i\in I} A_i = \{x \in A_i，对所有\ i \in I\}.$$

集族(1)中所有集合的并记为 $\bigcup_{i\in I} A_i$，即

$$\bigcup_{i\in I} A_i = \{x \in A_i, \text{对某个 } i \in I\}.$$

也就是说，交集是由所有 A_i 的公共元素组成，而并集把各个 A_i 的元素放在一起.

用 $A\times B$ 代表集合 A、B 的**笛卡尔积**，即

$$A \times B = \{(a, b) \mid a \in A, b \in B\},$$

这里，若 $a_1, a_2 \in A$，$b_1, b_2 \in B$，那么

$$(a_1, b_1) = (a_2, b_2)$$

当且仅当 $a_1 = a_2$，$b_1 = b_2$.

第一章　关系与运算

§1　映　射

设 A、B 是集合. 如果有一个对应规则 f，使得集合 A 中的每个元素 a 都对应 B 中一个确定的元素 b，则说这个对应 f 是从集合 A 到集合 B 的一个**映射**，记成

$$f: A \to B,$$
$$f: a \to b.$$

也写成 $f(a) = b$.

设 A 是个集合，规定

$$i_A: A \to A,$$
$$i_A: a \to a.$$

这个映射称为**恒等映射**，又因为人们习惯于把 A 到自身的映射称为 A 上**变换**，故 i_A 也称为 A 上**恒等变换**.

定义 1　设 f 是集合 A 到集合 B 的映射，称集合

$$\{y \in B \mid 有\ a \in A\ 使\ y = f(a)\}$$

为映射 f 的**象**，记为 $\mathrm{Img}(f)$，或 $f(A)$.

当 $\mathrm{Img}(f) = B$ 时，说 f 是满的，或说 f 是个**满射**.

当 A 中不同元素对应 B 中不同元素时，即 $a_1, a_2 \in A$, $a_1 \neq a_2$，则有 $f(a_1) \neq f(a_2)$，我们说 f 是单的，或者说 f 是**单射**.

如果 f 是单射又是满射，则说 f 是个**双射**.

定义 2　设 A, B, C 是集合，且 $f: A \to B$ 和 $g: B \to C$ 是映射. 规定，任意 $a \in A$ 对应 C 中元 $g(f(a))$，这是 A 到 C 的映射，称为 f, g 的**复合映射**，记为 $g \circ f$ 或 gf，即

$$g \circ f: A \to C,$$
$$g \circ f: a \to g(f(a)).$$

我们知道，两个映射

$$f_1: A_1 \to B_1, \quad f_2: A_2 \to B_2$$

相等的含 意是 $A_1 = A_2$, $B_1 = B_2$ 且对任意 $a \in A_1$ 恒有 $f_1(a) = f_2(a)$，也就是 f_1 和 f_2 对于 A_1 的每个元素作用相同.

命题 1 设 A、B、C、D 是集合，那么对任意映射

$$f: A \to B, \quad g: B \to C, \quad h: C \to D$$

恒有 $h \circ (g \circ f) = (h \circ g) \circ f$.

证明 容易看出 $h \circ (g \circ f)$ 和 $(h \circ g) \circ f$ 都是 A 到 D 的映射，且对任意 $a \in A$，有

$$h \circ (f \circ g)(a) = h(g \circ f)(a) = h(g(f(a)))$$
$$= h \circ g(f(a)) = (h \circ g) \circ f(a).$$

命题 2 设 A、B 是集合，$f: A \to B$ 是映射，则

$$f \circ i_A = i_B \circ f = f.$$

命题 3 设 A、B 是集合，$f: A \to B$ 是双射，则有 $g: B \to A$ 使

$$g \circ f = i_A, \quad f \circ g = i_B.$$

证明 由于 f 是满射，对于任意 $b \in B$，必有 $a \in A$ 使 $f(a) = b$，而 f 又是单的，故在 A 中有唯一确定的 a 使 $f(a) = b$，规定

$$g: B \to A,$$
$$g: b \to a, \quad f(a) = b,$$

g 是 B 到 A 的映射.

对任意 $b \in B$，设 $f(a) = b$，则 $g(b) = a$，故

$$f \circ g(b) = f(g(b)) = f(a) = b = i_B(b),$$

从而 $f \circ g = i_B$.

对任意 $a \in A$，设 $f(a) = b$，亦有 $g(b) = a$，故

$$g \circ f(a) = g(f(a)) = g(b) = a = i_A(a),$$

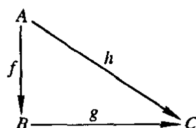
从而得 $g \circ f = i_A$.

对于复合映射使用图形语言有时是很方便的.

定义 3　设 A、B、C 是集合，若映射

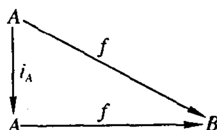
$$f: A \to B, \qquad g: B \to C, \qquad h: A \to C$$

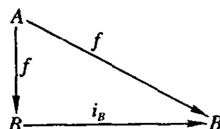
满足关系 $h = g \circ f$, 则说图形



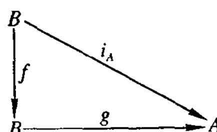
可换.

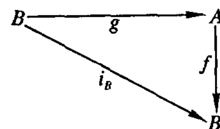
例如，命题 2 即图形



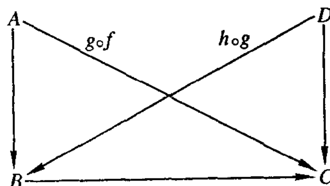


可换，而命题 3 就是图形





可换，命题 1 可以说是图形



可换.

习　题

1. 设 A, B, C 是集合

$$f: A \to B, \quad g: B \to C,$$

证明：

(1) 如果 f 和 g 都是满的，则 $g \circ f$ 亦然；

(2) 如果 f 和 g 都是单的，则 $g \circ f$ 亦然；

(3) 如果 $g \circ f$ 是满的，则 g 是满的；

(4) 如果 $g \circ f$ 是单的，则 f 是单的.

2. 条件如上题，举例：

(1) $g \circ f$ 是满的，但 f 不是满的；

(2) $g \circ f$ 是单的，但 g 不是单的.

3. 设 $f: A \to B$, $g: B \to C$, $h: B \to C$，且 $h \circ f = g \circ f$. 证明，若 f 是满射，则 $g = h$.

4. 设 $f: A \to B$, $g: A \to B$, $h: B \to C$，且 $h \circ f = h \circ g$. 证明，若 h 是单射，则 $f = g$.

5. 如果映射 $f: A \to B$ 和 $g: B \to A$ 满足

$$g \circ f = i_A, \qquad f \circ g = i_B.$$

证明，f 和 g 都是双射.

6. 设 f 是正整数集 $\mathbf{N}^*$ 上的变换 $f(m) = m + 1$. 证明，有无穷多个 $\mathbf{N}^*$ 上变换 g 使 $g \circ f = i_{\mathbf{N}^*}$，但没有 $\mathbf{N}^*$ 上变换 h 能使 $f \circ h = i_{\mathbf{N}^*}$.

§2　等价关系与分类

分类是许多学科经常采用的研究方法，一种科学的分类，使同类研究对象的共同属性更为明了，各类间的差别更为明晰，研究工作可以事半功倍.

本节把这种分类方法概括化、抽象化.

定义 1　设 A 是个非空集合，$\mathscr{R}$ 是笛卡尔积 $A\times A$ 的一个子集，若 $(a,b)\in\mathscr{R}$，则说 a，b 有关系 $\mathscr{R}$，记为 $a\mathscr{R}b$；若 $(a,b)\notin\mathscr{R}$，则说 a、b 没有 $\mathscr{R}$ 关系. $A\times A$ 的子集 $\mathscr{R}$ 称为 A 上**关系** $\mathscr{R}$.

例如，$A=\{1,2,3\}$，$\mathscr{R}=\{(1,2),(1,3),(2,3)\}$，则 $1\mathscr{R}2$，$1\mathscr{R}3$，$2\mathscr{R}3$.

例 1　实平面 $\mathbf{R}\times\mathbf{R}$ 中，由

$$x^2+y^2=1,$$
$$(x-1)^2+y^2=1$$

确定的两个圆周上的所有点构成的子集为 $\mathscr{S}$，则 $1\mathscr{S}0$，$0\mathscr{S}1$，$(-1)\mathscr{S}0$，$2\mathscr{S}0$，$1\mathscr{S}1$，….

例 2　设 $f\colon A\to A$，且

$$\mathscr{R}=\{(a,b)\in A\times A\mid b=f(a),\ a\in A\}.$$

那么，对每个 $a\in A$ 必有 A 中元 $f(a)$ 与 a 有 $\mathscr{R}$ 关系，即 $a\mathscr{R}f(a)$；当 f 是满射时，对于每个 A 中元 b 一定有元 a 与 b 有关系，即若 $b=f(a)$ 则 $a\mathscr{R}b$，这样的 a 可能不只一个；当 f 是双射时，对于每个 $a\in A$，有而且只有一个 $c\in A$ 使 $c\mathscr{R}a$.

定义 2　设 $\mathscr{R}$ 是 A 上一个关系，若满足

1. 反身性，即对任意 $a\in A$ 都有 $a\mathscr{R}a$；

2. 对称性，即对任意 a，$b\in A$，只要 $a\mathscr{R}b$，则必有 $b\mathscr{R}a$；

3. 传递性，即对任意 a，b，$c\in A$，只要 $a\mathscr{R}b$，$b\mathscr{R}c$，则必有 $a\mathscr{R}c$；则说 $\mathscr{R}$ 是个**等价关系**.

例 3　在整数集 $\mathbf{Z}$ 上，令

$$\mathscr{R}=\{(a,b)\in\mathbf{Z}\times\mathbf{Z}\mid a+b\text{ 为偶数}\}.$$

首先，对任意整数 a，$a+a$ 是个偶数，故 $a\mathscr{R}a$.

其次，对任意整数 a，b，若 $a\mathscr{R}b$，即 $a+b$ 为偶数，则 $b+a$ 为偶数，故 $b\mathscr{R}a$.

最后，对任意整数 a, b, c, 若 $a\mathscr{R}b$, $b\mathscr{R}c$, 即 $a+b$, $b+c$ 均为偶数，则 $a+c+2b$ 为偶数，从而 $a+c$ 为偶数，故有 $a\mathscr{R}c$.

于是，$\mathscr{R}$ 是一个等价关系.

在生活和学习中，我们熟悉的等价关系是很多的.

用 $M_{n\times n}(\mathbf{R})$ 代表所有 n 阶实方阵的集合，$M_{n\times n}(\mathbf{R})\times M_{n\times n}(\mathbf{R})$ 的子集 $\mathscr{R}_1$, $\mathscr{R}_2$, $\mathscr{R}_3$, $\mathscr{R}_4$, $\mathscr{R}_5$ 定义如下：

$(A, B)\in\mathscr{R}_1$ 当且仅当有 n 阶可逆阵 P, Q 使 $A=PBQ$;

$(A, B)\in\mathscr{R}_2$ 当且仅当有 n 阶可逆阵 P 使得 $A=P^{-1}BP$;

$(A, B)\in\mathscr{R}_3$ 当且仅当有 n 阶可逆阵 Q 使得 $A=Q'BQ$;

$(A, B)\in\mathscr{R}_4$ 当且仅当它们的迹数相等；

$(A, B)\in\mathscr{R}_5$ 当且仅当 $|A|=|B|$.

则它们都是等价关系.

又如，用 F 代表实平面上所有三角形的集合，且子集

$$\mathscr{R}=\{(\Delta_1, \Delta_2)\in F\times F\mid \Delta_1 \text{ 相似于 } \Delta_2\},$$

则 $\mathscr{R}$ 是个等价关系.

在我们提过的关系中，有些不是等价关系. 例如 $A=\{1, 2, 3\}$, $\mathscr{R}=\{(1, 2), (2, 3), (1, 3)\}$, 则 $\mathscr{R}$ 不满足反身性和对称性. 例 1 确定的关系 $\mathscr{P}$ 也不是等价关系.

设 A 是个集合，给定 $A\times A$ 的一个子集也就确定了 A 中元 a, b 满足的一个条件 $\mathscr{P}$, 即 $\mathscr{R}$ 总可写成

$$\mathscr{R}=\{(a, b)\in A\times A\mid a, b \text{ 满足 } \mathscr{P}\}$$

所以我们讨论子集 $\mathscr{R}$ 和讨论与 $\mathscr{R}$ 对应的性质 $\mathscr{P}$ 是一回事. 从而可将等价关系的定义换一种说法.

定义 3 设 A 是个非空集合，$\mathscr{P}$ 是一种性质，对于 A 的任意有序元对 a, b 而言，都可明确地说它们满足性质 $\mathscr{P}$ 或者不满足性质 $\mathscr{P}$. 若 a, b 满足 $\mathscr{P}$, 则说 a, b 有 $\mathscr{P}$ 关系；如果 a, b 不满足性质 $\mathscr{P}$, 则说 a, b 没有 $\mathscr{P}$ 关系.

当 a, b 有 $\mathscr{P}$ 关系时，记为 $a\mathscr{P}b$. 若 $\mathscr{P}$ 性质确定的 $\mathscr{P}$ 关系

有：

1. 对任意 $a \in A$ 都有 $a\mathscr{P}a$；

2. 对任意 $a, b \in A$，只要 $a\mathscr{P}b$ 则 $b\mathscr{P}a$；

3. 对任意 $a, b, c \in A$，只要 $a\mathscr{P}b$ 且 $b\mathscr{P}c$ 则必 $a\mathscr{P}c$.

则说 $\mathscr{P}$ 是 A 上的一个等价关系.

在讨论一个确定问题时，为了方便，有时把性质 $\mathscr{P}$ 虚化，用 ~ 代替.

例 4　设 V 是 n 维实线性空间，A 是 V 的幂集，对任意 $U, W \in A$，如果 U 的每个向量均可由 W 中有限个向量线性表示出来，且 W 的每个向量均可由 U 中有限个向量线性表示出来，则说 $U \sim W$. 容易证明，~ 是 A 上的一个等价关系.

例 5　记区间 $[0, 1]$ 上的所有连续函数构成的集合为 A，规定，对任意 $f(x), g(x) \in A$，$f(x) \sim g(x)$，当而且仅当

$$\int_0^1 f(x)\,\mathrm{d}x = \int_0^1 g(x)\,\mathrm{d}x,$$

则 ~ 是 A 上一个等价关系.

同样，在区间 $[0, 1]$ 上所有可微函数构成的集合 A 中，规定，对任意 $f(x), g(x) \in A$，$f(x) \sim g(x)$ 当而且仅当 $f'(x) = g'(x)$，也就是 $f(x) - g(x)$ 为常数，则 ~ 是 A 上一个等价关系.

等价关系与分类问题密切相关.

定义 4　设 ~ 是集合 A 上一个等价关系，对于每个 $x \in A$，称子集

$$S_x = \{y \in A \mid y \sim x\}$$

为由 x 确定的**等价类**.

例如，在例 3 给出的 $\mathbf{Z}$ 上等价关系，即 $a \sim b$，当且仅当 $a + b$ 为偶数，那么

$$S_1 = \{\cdots, -1, 1, 3, \cdots\},$$

$$S_2 = \{\cdots, -2, 0, 2, 4, \cdots\},$$

且 $S_1=S_3=S_5$，$S_0=S_{-2}=S_2$.

命题 1 设 A 是个非空集合，$\sim$ 是 A 上的一个等价关系，用 S_x 代表 x 在 $\sim$ 之下确定的等价类，那么：

1. 对任意 $x\in A$，等价类 S_x 非空；
2. 对任意 x，$y\in A$，若 $S_x\neq S_y$，必 $S_x\cap S_y=\varnothing$；
3. A 恰为所有不相同的等价类的并集.

证明 对任意 $x\in A$，由于 $\sim$ 是等价关系，有反身性，即 $x\sim x$，故 $x\in S_x$，$S_x\neq\varnothing$.

如果 x，$y\in A$，且 $S_x\cap S_y\neq\varnothing$，可设 $z\in S_x\cap S_y$，则 $z\sim x$，$z\sim y$，从而 $x\sim y$，进而 $x\in S_y$，再用传递性得 $S_x\subseteq S_y$，对称地可得 $S_y\subseteq S_x$，最后得 $S_x=S_y$. 这说明 S_x 和 S_y 或相同或不相交.

由于每个 $x\in A$ 均有 $x\in S_x$，故 $A=\bigcup\limits_{x\in A}S_x$. 把其中相同的等价类剔除，则 A 即为两两不交的等价类的并集.

一个集合 Δ，有以 I 为标号集的子集族

$$\{T_i\subseteq\Delta\mid i\in I\},$$

满足：

1. 对任意 $i\in I$，$T_i\neq\varnothing$；
2. 对任意 i，$j\in I$，当 $i\neq j$ 时，$T_i\cap T_j=\varnothing$；
3. $\Delta=\bigcup\limits_{i\in I}T_i$；

则说这个子集族给出集合 Δ 的一个**分类**.

命题 2 若集合 Δ 由子集族

$$\{T_i\subseteq\Delta\mid i\in I\}$$

决定一个分类. 规定，任意 a，$b\in\Delta$，$a\sim b$ 当而且仅当 a，b 属于同一个 T_i，则 $\sim$ 是 Δ 上一个等价关系.

证明 该分类是确定的，从而对任意 a，$b\in\Delta$ 而言，a，b 或者在同一个子集内或者分属不同子集，即 $a\sim b$ 或 a，b 没有 $\sim$ 关系是明确的. $\sim$ 是 Δ 上一个关系.

对任意 $a\in A$，必有 $i\in I$ 使 $a\in T_i$，从而可以说 a，a 在 T_i 中，即 $a\sim a$，$\sim$具有反身性.

对任意 a，$b\in A$，若 $a\sim b$，即有 $i\in I$ 使

$$a\in T_i,\qquad b\in T_i,$$

当然有 $b\sim a$，即$\sim$有对称性.

设 $a\sim b$，$b\sim c$，即有 $i,j\in I$ 使

$$a,b\in T_i,\qquad b,c\in T_j,$$

由于在分类中 b 属于唯一确定的 T_i，可知必有 $i=j$，a，$c\in T_i$，$a\sim c$. $\sim$具传递性.

这样就把分类与等价关系对应起来了.

例 6 看例 5 的第二个例子，由 $f'(x)=g'(x)$确定 $f(x)\sim g(x)$，从而得 A 的一个分类. 对任意可微函数 $f(x)$，

$$S_{f(x)}=\{g(x)\in A\mid g'(x)=f'(x)\},$$

且

$$A=\bigcup_{f(x)\in A}S_{f(x)}.$$

这种表达中的等价类有些是重复的.

例 7 看例 2 之等价关系，它把整数集分成两个等价类，即 $\mathbf{Z}$ 是奇数集与偶数集之并

$$\mathbf{Z}=S_1\cup S_2.$$

这种写法中无重复项.

定义 5 设$\sim$是集合 A 上的一个等价关系，T 是 A 的一个子集，如果 T 中不同的元素的等价类一定不同，且 $A=\bigcup\limits_{t\in T}S_t$，则 T 是关系$\sim$之下的**完全集**.

若 T 是等价关系$\sim$之下的一个完全集，则称集合

$$\bar{A}=\{S_t\mid t\in T\}$$

为等价关系$\sim$的**商集**，有时记 $\bar{A}=A/\sim$.

对于一个等价关系$\sim$可能有很多不同的完全集，例 3 中

$$\{0,1\},\quad \{1,2\},\quad \{-1,100\}$$

都是完全集.

但由 ~ 决定的商集是唯一确定的，与完全集的选择无关，$A/\sim$ 乃是其所有不同的等价类构成的集合. 例 3 中

$$\mathbf{Z}/\sim = \{S_0, S_1\} = \{S_1, S_2\},$$

因为 S_0 和 S_2 是相同的集合，都是偶数集.

又如，在例 5 中，我们用常数 c 代表函数

$$f(x) = c, \qquad x \in [0,1],$$

则实数集 $\mathbf{R}$ 是所说等价关系 ~ 的一个完全集. 因为 $\{S_c \mid c \in \mathbf{R}\}$ 包含了所有不同的等价类. 当然，所有过原点的直线函数 cx 也构成一个完全集

$$\{S_{cx} \mid c \in \mathbf{R}\}.$$

因为，若 $f(x)$ 是 $[0,1]$ 上连续函数，且

$$\int_0^1 f(x)\,dx = b,$$

则 $f(x) \sim 2bx$，即 $f(x) \in S_{2bx}$. 且不同的直线的等价类不同.

再如，在 $M_{n\times n}(\mathbf{R})$ 中规定 $A \sim B$ 当而且仅当有 n 阶可逆阵 P，Q 使得 $A = PBQ$，那么，~ 是个等价关系. 学过线性代数后知道，$A \sim B$ 的充要条件是它们秩数相同，故

$$\left\{\begin{pmatrix}0 & & & & \\ & 0 & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 0\end{pmatrix}, \begin{pmatrix}1 & & & & \\ & 0 & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 0\end{pmatrix}, \begin{pmatrix}1 & & & & \\ & 1 & & & \\ & & 0 & & \\ & & & \ddots & \\ & & & & 0\end{pmatrix}, \cdots, \begin{pmatrix}1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1\end{pmatrix}\right\}$$

是~之下的一个完全集，而

$$M_{n\times n}(\mathbf{R})/\sim=\{T_0, T_1, \cdots, T_n\},$$

其中 T_i 是所有秩数为 i 的 n 阶方阵的集合.

习　题

1. 用 $A\times A$ 的子集 $\mathscr{R}$ 表达下列关系：

(1) $A=\{1, 2, 3, 4, 5\}$，当 $a<b$ 时，说 a, b 有 $\mathscr{R}$ 关系；

(2) $A=\{2, 3, 4, 5\}$，当 a, b 互素时，说 a, b 有 $\mathscr{R}$ 关系；

(3) $A=\{3, 6, 9, 12\}$，当 a 整除 b 时，说 a, b 有 $\mathscr{R}$ 关系.

2. 给出一个关系，它有对称性、传递性但无反身性；给出一个关系，它有反身性、传递性但无对称性. 给出一个关系，它有反身性、对称性但无传递性.

3. 设 A 是非空集合，且对每个正整数 i

$$\mathscr{R}_i\subseteq A\times A,$$

均确定一个等价关系. 证明，如果对任意 i 恒有 $\mathscr{R}_i\subseteq\mathscr{R}_{i+1}$，则并集 $\mathscr{R}=\bigcup\limits_{i=1}^{\infty}\mathscr{R}_i$ 也确定一个等价关系.

4. 设 n 是一个正整数，在 $\mathbf{Z}$ 上规定整数 $a\sim b$ 当而且仅当 n 整除 $a-b$. 证明~是个等价关系，给出 $\mathbf{Z}/\sim$.

§3　运　算

我们已经接触过很多运算，如数的乘法、矩阵的加法、向量的加法、多项式的结式等等. 它们有什么共同的性质呢？抽象代数学中所要研究的运算的对象不再是简单的数字而是任意集合.

定义 1　设 S 是个非空集合，把 $S\times S$ 到 S 的映射 f 称为是

S 上的一个**二元运算**，有时简称为一个**乘法**，且简记 $f(x, y) = xy$.

容易看出，数的加法、减法、乘法是整数集上的运算，也是有理数集、实数集、复数集上的运算.

数的减法不是正整数集 $\mathbf{N}^*$ 上的运算，因为它不能指明整数 2, 3 在 $\mathbf{N}^*$ 中对应何元.

在有理数集 $\mathbf{Q}$ 上，中学里讲的"除法"不符合这里关于运算的定义，因为 $(0, 0) \in \mathbf{Q} \times \mathbf{Q}$ 但不对应任何有理数.

例 1 在正整数集 $\mathbf{N}^*$ 上，规定 $(m, n) \in \mathbf{N}^* \times \mathbf{N}^*$ 对应 m 的 n 次幂 m^n，这是 $\mathbf{N}^*$ 的一个运算.

例 2 设 A 是一个集合，$M(A)$ 是由所有 A 到 A 的映射构成的集合，规定，对任意 $(f, g) \in M(A) \times M(A)$，对应 $g \circ f \in M(A)$，则得到 $M(A)$ 上一个运算.

当 A 为 n 元集时，不妨简记

$$A = \{1, 2, \cdots, n\},$$

而把 A 到 A 的双射记为置换

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix},$$

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix},$$

当然 τ 也可以写成

$$\tau = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \tau\sigma(1) & \tau\sigma(2) & \cdots & \tau\sigma(n) \end{pmatrix},$$

则规定置换 σ, τ 对应置换

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau\sigma(1) & \tau\sigma(2) & \cdots & \tau\sigma(n) \end{pmatrix}.$$

这是变换"复合"运算的一种特殊情形.

例 3 设 A 是一个集合，S 是 A 的幂集. 规定，对任意

$(U, V) \in S \times S$，对应 $U \cap V$，则得到 S 的一个运算．若规定 (U, V) 对应 $U \cup V$，也得到 S 的一个运算．

对于有限集 A，可以把 $A \times A$ 的所有元素及其对应元列出来．这样的表称为运算表．

例 4　集合{好，坏}上，规定

(好，好)→好，　(好，坏)→坏，

(坏，好)→坏，　(坏，坏)→坏．

其运算表是

·	好	坏
好	好	坏
坏	坏	坏

定义 2　设·是集合 A 上的一个运算，若对任意 $a, b, c \in A$，都有

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

则说运算·满足**结合律**，若对任意 $a, b \in A$，都有

$$a \cdot b = b \cdot a,$$

则说·满足**交换律**．

整数集、有理数集、实数集上的加法和乘法都满足结合律和交换律，但减法运算不满足结合律，也不满足交换律．

在矩阵集 $M_{n \times n}(\mathbf{R})$，规定

$$((a_{ij}), (b_{ij})) \in M_{n \times n}(\mathbf{R}) \times M_{n \times n}(\mathbf{R})$$

对应 (c_{ij})，其中

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj},$$

则得 $M_{n \times n}(\mathbf{R})$ 的一个运算，就是线性代数学中的矩阵乘法，它满足结合律但不满足交换律．

例 1 中的运算不满足结合律，因为

$$(2\cdot 1)\cdot 2=2^1\cdot 2=2^2=4,$$
$$2\cdot(1\cdot 2)=2\cdot 1^2=2^1=2.$$

例5　在$M_{n\times n}(\mathbf{R})$上规定，任意$A$，$B\in M_{n\times n}(\mathbf{R})$对应$A\cdot B=A+B-AB$，则运算·满足结合律.

证明　对任意n阶实矩阵A，B，C，有

$$\begin{aligned}&(A\cdot B)\cdot C\\&=(A+B-AB)\cdot C\\&=A+(B-AB+C)-(A+B-AB)C\\&=A+B+C-AB-AC-BC+(AB)C,\\&A\cdot(B\cdot C)\\&=A\cdot(B+C-BC)\\&=A+(B+C-BC)-A(B+C-BC)\\&=A+B+C-BC-AB-AC+A(BC).\end{aligned}$$

故$(A\cdot B)\cdot C=A\cdot(B\cdot C)$.

数的运算中，数字0和1地位很重要．因为对任意数a而言

$$a+0=a,\qquad 1a=a.$$

同样的事情在矩阵的加法、乘法，函数的加法、乘法，变换的复合中也可以见到．基于这样的背景，有

定义3　设·是集合A上的一个运算，如果有$e\in A$对任意$a\in A$恒有

$$e\cdot a=a\cdot e=a$$

则说e是A在运算·之下的一个**恒等元**，也说是**单位元**.

例如，n阶单位矩阵是$M_{n\times n}(\mathbf{R})$在矩阵乘法之下的一个单位元．零矩阵是$M_{n\times n}(\mathbf{R})$在矩阵加法之下的一个单位元.

例4中的集合{好，坏}在所指的乘法之下，元素“好”是个单位元.

例3中集合A的幂集S中的元素A在运算∩之下是个恒等

元，因为，对任意 $V\in S$，即 $V\subseteq A$ 恒有

$$A\cap V=V\cap A=V.$$

同理，S 的元素空集 $\varnothing$ 在运算 $\cup$ 之下是一个恒等元，因为，对任意 $V\in S$，即 $V\subseteq A$，有

$$V\cup\varnothing=\varnothing\cup V=V.$$

在正整数集 $\mathbf{N}^*$ 上规定 m，$n\in\mathbf{N}^*$ 对应 m 的 n 次幂 m^n，即

$$m\cdot n=m^n,$$

则任何元素都不是 · 的单位元，否则，可由

$$e\cdot 2=e^2=2^e=2\cdot e=2$$

推出 $e=1$，$1^2=2$ 矛盾.

命题 3　对于集合 A 上的运算 · 而言，如果有恒等元，则必唯一.

证明　如果 e,f 都是 A 在 · 之下的恒等元，由于 e 是恒等元，应有

$$e\cdot f=f\cdot e=f,$$

但 f 也是恒等元，又应有

$$f\cdot e=e\cdot f=e,$$

故

$$e=f.$$

使用矩阵工具时都知道，若 n 阶矩阵 A 可逆，也就是有 n 阶阵 B 使 $AB=BA=I_n$，则当 A 出现在线性方程组中或出现在矩阵方程中，就可以在等式两端搬来搬去（乘逆矩阵 A^{-1}），十分方便，对于这种元素理应予以特别注意.

定义 4　设 · 是集合 A 上的一个运算，e 是 · 之下的恒等元，a 是 A 的一个元素，如果有元素 $b\in A$ 使

$$a\cdot b=b\cdot a=e$$

则说 a 是 A 的在 · 之下的一个**可逆元**，b 是 a 的一个**逆元素**.

例如，整数集 $\mathbf{Z}$ 在数的加法之下数 0 是恒等元（必唯一）.

数 -2 是数 2 的一个逆元.

n 阶置换的集合 A 在置换乘法之下，恒等置换是个单位元(必唯一)，且每个置换

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

都可逆，置换

$$\begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$$

是它的一个逆元.

命题 4 设集合 A 上的运算 $\cdot$ 满足结合律且有恒等元 e，$a \in A$. 如果 a 有逆元，则必唯一.

证明 如果 b, c 都是 a 的逆元，即

$$b \cdot a = a \cdot b = e,$$

$$c \cdot a = a \cdot c = e,$$

那么，必有

$$(c \cdot a) \cdot b = e \cdot b = b = c \cdot (a \cdot b) = c \cdot e = c.$$

习题

1. 在整数集 $\mathbf{Z}$ 上，规定

$$m \cdot n = 2m + n^2, \quad 任意\ m, n \in \mathbf{Z}$$

证明，运算 $\cdot$ 不满足结合律，不满足交换律，也没有恒等元.

2. 给出例 5 中运算 $\cdot$ 的一个恒等元.

3. 设 $\cdot$ 是集合 A 上的一个运算，且满足结合律. S 是 A 的幂集. 规定，S 的任意元 B, C(也就是 A 的二个任意子集)，对应 S 的元

$$B \times C = \{a \cdot b \in A \mid a \in B, b \in C\}.$$

证明，运算 $\times$ 满足结合律.

4. 设 $A = \{0, 1\}$，其运算表是

×	0	1
0	0	1
1	1	0

证明，运算×满足结合律和交换律，而且有恒等元，且每个元都有逆元.

第二章　群

一个集合带有一个运算，此运算满足结合律，再加上有恒等元及每元均可逆的要求，就成为一个群. 数学、物理学、化学、生物学，甚至社会科学中很多研究对象经抽象化后，表现出的最基本的数学结构特点就是它们是一个群.

这个抽象过程，数学上称为公理化. 满足群的定义的几条公理的任何系统都是群论的研究对象. 在公理之下演绎出来的命题、定理对它们都适用. 我们得到的一般原则就可以指导每一个具体的群的研究.

§1　群的定义

定义 1　一个集合 G 和 G 上一个运算 $\cdot$ 满足如下条件:

(1) 运算 $\cdot$ 满足结合律;

(2) 有恒等元 e;

(3) G 的每个元都有逆元;

则说 $(G, \cdot)$ 是个群，在不致引起混淆时，可把特指的运算 $\cdot$ 省略不提，而简单说 G 是个群.

例如，用 $+$ 代表数的加法，$\times$ 代表数的乘法，$\mathbf{R}^+$ 代表所有正实数的集合，$A=\{1, -1\}$，则

$$(\mathbf{Z}, +), (\mathbf{R}, +), (\mathbf{R}^+, \times), (A, \times)$$

都是群.

所有 n 元置换构成的集合，在置换的乘法(即复合之下)是个群，通常称为 **n 阶对称群**.

例 1　用$M(A)$代表非空集A上所有双射变换构成的集合，用·代表映射复合，则$(M(A),\ \cdot)$是个群.

例 2　用S代表数域Ω上所有n阶可逆矩阵构成的集合，用·代表矩阵乘法，则$(S,\ \cdot)$是个群，称为Ω上n阶完全线性群.

例 3　上节习题之第 4 题$(\{0,\ 1\},\ \cdot)$是个群，它在电子计算机和逻辑学中代表两种状态间的一种相互作用.

例 4　对任意给定的实数对$(a,\ b)$，$a\neq 0$，用$f_{a,b}$代表$\mathbf{R}$到$\mathbf{R}$的变换

$$f_{a,b}:\ \mathbf{R}\rightarrow\mathbf{R},$$

$$f_{a,b}:\ x\rightarrow ax+b,$$

所有这样的变换构成的集合记为A，则A在变换的复合运算$\circ$之下构成一个群.

首先，要说明"复合"确实是A上的运算. 任取$(a,\ b)$和$(c,\ d)$，$a\neq 0$，$c\neq 0$，则

$$\begin{aligned}(f_{a,b}\circ f_{c,d})(x)&=f_{a,b}(f_{c,d}(x))\\&=f_{a,b}(cx+d)=acx+(ad+b),\end{aligned}$$

且$ac\neq 0$，故

$$f_{a,b}\circ f_{c,d}=f_{ac,cd+b}\in A,$$

即$\circ$是A上的运算.

其次，$f_{1,0}(x)=x=i_{\mathbf{R}}(x)$，故$f_{1,0}$是$A$的恒等元.

最后，对任意$f_{a,b}\in A$，即$(a,\ b)\in\mathbf{R}\times\mathbf{R}$，$a\neq 0$，看由$(a^{-1},\ -a^{-1}b)$决定的变换$g=f_{a^{-1},\,-a^{-1}b}$，则

$$g\circ f_{a,b}=f_{a,b}\circ g=f_{1,0}.$$

总之，$(A,\ \circ)$是个群.

在第一章§3，我们已经知道，如果A上运算·满足结合律，有恒等元e，那么，A的任意可逆元只能有唯一一个逆元. 在群$(G,\ \cdot)$中，每个元g都有逆元，它由g唯一确定，今后就

记为 g^{-1}. 同时，群$(G,\ \cdot)$中两个元素 a，b 的运算结果 $a\cdot b$ 简记为 ab，而说到群$(G,\ \cdot)$时可不特别指明该运算，而简说 G 是个群·.

命题 1 设 G 是个群，a，$b\in G$，则 a^{-1}的逆元恰为 a，ab 的逆元恰为 $b^{-1}a^{-1}$，即

$$(a^{-1})^{-1}=a,\qquad (ab)^{-1}=b^{-1}a^{-1}.$$

证明 作为 G 的一个元素 a^{-1}，有 a 使

$$aa^{-1}=a^{-1}a=e,$$

故 a 为 a^{-1}的逆元，也就是 $a=(a^{-1})^{-1}$.

对于元素 ab，因为

$$(b^{-1}a^{-1})(ab)=b^{-1}(a^{-1}a)b=b^{-1}b=e,$$

$$(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=aa^{-1}=e,$$

故 $b^{-1}a^{-1}$就是 ab 的逆元，$(ab)^{-1}=b^{-1}a^{-1}$.

推论 如果 G 是个群，g_1，…，$g_n\in G$，则

$$(g_1g_2\cdots g_n)^{-1}=g_n^{-1}\cdots g_1^{-1}.$$

命题 2 设 G 是个群. 对任意 a，b，$c\in G$，如果 $ab=ac$，则必有 $b=c$.

事实上，在 $ab=ac$ 的两端同时从左方乘以 a^{-1}，则得到

$$a^{-1}(ab)=a^{-1}(ac),\qquad b=c.$$

这说明群中乘法满足左消去律. 同样，也满足右消去律.

定理 1 设·是非空集合 G 上的一个运算且满足结合律，那么，$(G\cdot)$是个群当而且仅当对任意 a，$b\in G$ 都有唯一确定的 c，$d\in G$ 使

$$a\cdot c=b,\quad d\cdot a=b. \tag{1}$$

证明 如果$(G,\ \cdot)$是个群，那么，对任意 a，$b\in G$，令

$$c=a^{-1}\cdot b,\quad d=b\cdot a^{-1},$$

则

$$a\cdot c=a\cdot a^{-1}\cdot b=b,$$

$$d \cdot a = b \cdot a^{-1} \cdot a = b.$$

而由左、右消去律知 a, d 唯一.

反之，如果对任意 $a, b \in G$ 都有 c, d 满足等式(1). 因为 G 非空，可任取一 $g \in G$, 对于 g, g 必有 e 使 $e \cdot g = g$. 而对于任意 $x \in G$, 又应有 h 使 $x = g \cdot h$, 从而

$$e \cdot x = (e \cdot g) \cdot h = g \cdot h = x.$$

对称地，可以得到一个元素 f, 对任意 $x \in G$ 都有 $x \cdot f = x$. 由 e, f 之特性可知

$$e = e \cdot f = f,$$

即 e 为 G 之恒等元.

对于任意 $a \in G$, 应有 b, c, 使

$$b \cdot a = e, \qquad a \cdot c = e,$$

再由

$$(b \cdot a) \cdot c = e \cdot c = c = b \cdot (a \cdot c) = b$$

知 $b = c$ 就是 a 的逆元.

$(G, \cdot)$是个群.

通常把群的运算称为乘法，e 代表恒等元.

由于群的乘法满足结合律，取群的一个元素 a, a 乘 a 记成 a^2, $aa \cdots a$ 为 n 个 a 相乘，则记为 a^n. 还规定 $a^{-n} = (a^n)^{-1}$, $n > 0$, 及 $a^0 = e$. 则有

命题 3　设 a 是群 G 的任意元，n 为一正整数，则

$$a^{-n} = (a^{-1})^n.$$

事实上 $a^{-n} = (a^n)^{-1}$, 而

$$\begin{aligned} a^n(a^{-1})^n &= a^{n-1}aa^{-1}(a^{-1})^{n-1} \\ &= a^{n-1}(a^{-1})^{n-1} = e, \end{aligned}$$

这说明$(a^{-1})^n$ 是 a^n 的逆元(另一侧的验算是平行的)，也就是

$$(a^{-1})^n = (a^n)^{-1} = a^{-n}.$$

命题 4　设 a 是群 G 的任意元，m, n 为任意整数，则

$$a^m a^n = a^{m+n}, \qquad (a^n)^m = a^{nm} = (a^m)^n.$$

证明 若 $m=0$，则 $a^0=e$，有

$$a^m a^n = ea^n = a^n = a^{m+n},$$

$$(a^n)^m = e = a^0 = a^{mn}.$$

若 m，n 都是正的，则 $a^m a^n$ 为 m 个 a 乘 n 个 a，等于 $m+n$ 个 a 相乘，即

$$a^m a^n = a^{m+n}.$$

而 $(a^n)^m$ 是 m 个 a^n 相乘，每个 a^n 又是 m 个 a 相乘，总的结果是 mn 个 a 相乘，故

$$(a^m)^n = (a^n)^m = a^{mn}.$$

当 m，n 均小于零时，由于

$$a^m = (a^{-1})^{-m}, \qquad a^n = (a^{-1})^{-n}.$$

计算 a^{-1} 的个数，即得所要的等式.

当 m 为正数，n 为负数时，令 $l=-n$，则

$$a^n = a^{-l} = (a^{-1})^l,$$

计算 $a^m a^n$ 中 a 和 a^{-1} 的个数，就有

$$a^m a^n = a^{m+n}.$$

而且还有

$$(a^n)^m = ((a^{-1})^l)^m = (a^{-1})^{lm} = a^{nm}.$$

当 m 为负数，n 为正数时，可仿上证之.

定义 2 如果群 G 的运算满足交换律，则称此群为**交换群**、**Abel 群**或**加法群**.

交换群的运算通常称为加法，记为 +，其恒等元称为**零元**，记为 0，元素 a 的逆元称为 a 的**负元**，记为 $-a$.

推论 设 a，b 是交换群 G 的任意元，m，n 是任意整数，则

$$m(-a) = (-m)a = -ma,$$

$$(m+n)a = ma + na,$$

$$(mn)a = m(na),$$
$$n(a+b) = na + nb.$$

习　　题

1. 设 F 是定义在 $(-\infty, \infty)$ 上的所有实函数的集合，规定，任意 $f, g \in F$，对应函数

$$f\#g: x \to f(x) + g(x), \quad x \in \mathbf{R}.$$

证明，$(F, \#)$ 是个交换群.

2. 设 $(G, \cdot)$ 是个群，完成下面乘法表，并说明此表的填法是唯一确定的：

$\cdot$	a	b	c
a		b	
b			
c			

3. 在整数集 $\mathbf{Z}$，规定，任意 $a, b \in \mathbf{Z}$ 对应

$$a * b = a + b - 2,$$

证明，$(\mathbf{Z}, *)$ 是个群.

4. 用 G 代表除 1 以外所有实数构成的集合，规定，对任意 $x, y \in G$，

$$x * y = x + y - xy,$$

证明 $(G, *)$ 是个群.

5. 设 x, y 是群 G 的元素，且

$$x^{-1}yx = y^{-1}, \qquad y^{-1}xy = x^{-1},$$

证明，$x^4 = y^4 = e$.

6. 设 G 是个有限集，其上运算 $\cdot$ 满足结合律，且满足左、右消去律，证明 $(G, \cdot)$ 是个群.

§2 子 群

定义 1 设$(G,\ \cdot)$是个群，H是G的一个非空子集. 如果$\cdot$也是H上的运算，且$(H,\ \cdot)$也构成群，则说这个群是$(G,\ \cdot)$的**子群**.

例如，整数加群是有理数加群的子群，也是复数加群的子群.

又如，所有实的 2 阶可逆阵作成的乘法群G中，由矩阵

$$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix},\quad \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix},\quad \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix},\quad \begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}$$

组成的集合H也在该种乘法之下构成群.

定义 1 中要求群G的运算$\cdot$也是集H上的运算，实际上即要求对任意$a, b\in H$总有$a\cdot b\in H$，这个运算在H上自然地满足结合律. 因此，我们要验证H是$(G,\ \cdot)$的子群，一般说来，比无任何基础地直接验证$(H,\ \cdot)$是个群要容易一些.

命题 1 如果H是G的子群，那么G的恒等元e必然属于H.

事实上，H是个群，设f为其恒等元，则$f^2=f$. 但e是G的恒等元，必有$fe=f$. 于是在G中将$f^2=f=fe$从左端消去f，即得$e=f$.

定理 1 设$(G,\ \cdot)$是个群，H是G的非空子集，那么H是G的子群，当而且仅当

(1) 如果$a, b\in H$，则$a\cdot b\in H$；

(2) 如果$a\in H$，则a在G中的逆元a^{-1}属于H.

证明 若H是$(G,\ \cdot)$的子群，则$\cdot$是H上运算，故满足(1).

又由命题 1 知$(G,\ \cdot)$的恒等元e就是群$(H,\ \cdot)$的恒等

元，故对任意 $a \in H$，必有 $b \in H$ 使

$$a \cdot b = b \cdot a = e,$$

但在 G 中 a 有逆 a^{-1} 使

$$a^{-1} \cdot a = a \cdot a^{-1} = e,$$

从而知

$$b = b \cdot a \cdot a^{-1} = (b \cdot a)a^{-1} = a^{-1}, \quad a^{-1} \in H.$$

设 G 的非空子集 H 满足(1)和(2)，则 · 也是 H 上的运算. 它自然满足结合律.

H 非空，设 $h \in H$. 由(2)知 h 知 G 中的逆元 $h^{-1} \in H$，再由(1)知 $h \cdot h^{-1} = e \in H$. H 有恒等元.

对任意 $a \in H$，由(2)知 $a^{-1} \in H$

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

即 H 的每个元在 H 中都有逆.

所以，$(H, \cdot)$ 是个群.

例 1　在所有非零有理数作成的乘法群 $\mathbf{Q}^*$ 中，形如

$$2^m 3^n, \ m, n \in \mathbf{Z}$$

的集合 H 是 $\mathbf{Q}^*$ 的一个子群.

H 显然非空.

任取 $2^m 3^n$，$m, n \in \mathbf{Z}$ 及 $2^i 3^j \in H$，$i, j \in \mathbf{Z}$，则

$$2^m 3^n \cdot 2^i 3^j = 2^{m+i} 3^{n+j} \in H.$$

对任意 $2^m 3^n \in H$，显然 $2^{-m} 3^{-n} \in H$.

H 是 $\mathbf{Q}^*$ 的一个子群.

定理 2　设 $(G, \cdot)$ 是个群，H 是 G 的一个非空子集. 那么，H 是 G 的子群的充分必要条件是对任意 $a, b \in H$，必有 $a \cdot b^{-1} \in H$.

证明　若 H 是 G 的子群，对任意 $a, b \in H$，由定理 1 知 $b^{-1} \in H$，进一步又有 $a \cdot b^{-1} \in H$.

反之，若对任意 $a, b \in H$ 都有 $a \cdot b^{-1} \in H$，由 H 非空，取 g

$\in H$，则知 $g \cdot g^{-1} = e \in H$.

对任意 $a \in H$，可推出 $e \cdot a^{-1} = a^{-1} \in H$.

对任意 $a, b \in H$，先推出 $b^{-1} \in H$，而对于 a, b^{-1} 又应有

$$a \cdot (b^{-1})^{-1} = a \cdot b \in H.$$

由定理 1 知 H 为 G 的子群.

例 2 G 是实的 n 阶完全线性群，H 是其行列式值为 1 的元素构成的子集，则 H 是 G 的一个子群.

事实上，若 $A, B \in G$，$|A| = 1$，$|B| = 1$，则 $|B^{-1}| = 1$. 从而 $|A||B^{-1}| = 1$，也就是 $AB^{-1} \in H$，H 是 G 的子群.

命题 2 设 G 是个群，则子集

$$C = \{a \in G \mid ax = xa, \text{对任意 } x \in G\}$$

是 G 的一个子群(称为 G 的中心).

证明 由于 $ae = ea$，故 $e \in C$，C 非空.

如果 $a, b \in C$，那么，对任意 $x \in G$，有

$$ax = xa, \qquad bx = xb,$$

将第二个等式左乘 b^{-1}，再右乘 b^{-1}，可知

$$xb^{-1} = b^{-1}x,$$

于是有

$$(ab^{-1})x = a(b^{-1})x = (ax)b^{-1} = x(ab^{-1}),$$

这说明 $ab^{-1} \in C$，C 是 G 的子群.

命题 3 设 G 是个群，且有子群族

$$\{H_i \mid i \in I\},$$

则交集 $H = \bigcap_{i \in I} H_i$ 也是 G 的一个子群.

证明 G 之恒等元 e 属于其每个子群 H_i，故 $e \in H$，H 非空.

如果 $a, b \in H$，则 $a, b \in H_i$，$i \in I$. 但每个 H_i 都是 G 的子群，故

$$ab^{-1} \in H_i, \quad i \in I,$$

进而 $ab^{-1} \in \bigcap\limits_{i \in I} H_i = H$. H 为 G 的子群.

可用 $H \leqslant G$ 表示 H 是 G 的子群.

定义 2　设 G 是个群，S 是 G 的一个非空子集，则称子群族

$$\{H \leqslant G \mid H \supseteq S\}$$

的交集为 G 的由 S **生成的子群**，记为 $\langle S \rangle$.

由于 G 本身就是一个包含 S 的子群，故定义 2 中的子群族非空，由命题 3 知 S 确定一个子群 $\langle S \rangle$.

当 $S = \{a_1, \cdots, a_n\}$ 是有限集时，记

$$\langle S \rangle = \langle a_1, a_2, \cdots, a_n \rangle.$$

例 3　设 G 是个群，$a \in G$，则

$$\langle a \rangle = \{\cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots\}.$$

事实上，G 的子集 $A = \{a^i \mid i \in I\}$ 中任意元 a^i, a^j 均使

$$a^i (a^j)^{-1} = a^i a^{-j} = a^{i-j} \in A.$$

这说明 A 是 G 的一个包含 a 的子群.

对于 G 的任意一个含 a 的子群 H，H 必然包含 e, a^{-1}, a^2, $\cdots$，即 $A \leqslant H$. 故子群族

$$\{H \leqslant G \mid a \in H\}$$

的交集包含 A，而 A 又是该族中一员，所以 $A = \langle a \rangle$.

例 4　设 G 是实的 3 阶完全线性群，求它的由下列三元素生成的子群 H

$$X = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, Y = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

用数学归纳法容易证明

$$X^n = \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, Y^m = \begin{pmatrix} 1 & 0 & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, m, n \in \mathbf{Z},$$

而 Z 与 X 类似，很容易看出相应性质.

实际上，X，Y，Z 都是初等矩阵，用它们右乘一个矩阵等于将该阵的某列加到另一列上去，有

$$X^n Z^m = \begin{pmatrix} 1 & n & mn \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} \in H, \text{任意 } m, n \in \mathbf{Z}$$

而对任意 $t \in \mathbf{Z}$，又有

$$\begin{pmatrix} 1 & n & mn \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n & t+mn \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix}.$$

故，对任意 m，n，$p \in \mathbf{Z}$，恒有

$$\begin{pmatrix} 1 & n & p \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix} \in H. \tag{1}$$

另一方面，所有形如(1)的矩阵的集合是 G 的一个子群(见习题)，故

$$\langle X, Y, Z \rangle = \left\{ \begin{pmatrix} 1 & n & p \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix}, n, m, p \in \mathbf{Z} \right\}.$$

例 5 设 G 是 n 阶对称群，T 是 $\{1, \cdots, n\}$ 的一个子集. 那么

$$H = \{\sigma \in G \mid \sigma(t) = t, \text{对每个 } t \in T\},$$
$$K = \{\sigma \in G \mid \sigma(T) = T\},$$

都是 G 的子群.

对任意 σ，$\tau \in H$ 及 $t \in T$，有

$$\sigma\tau^{-1}(T) = \sigma(\tau^{-1})(t)) = \sigma(t) = t.$$

故 $\sigma\tau^{-1} \in H$.

而对任意 σ，$\tau \in K$，由于

$$(\sigma\tau^{-1})(T) = \sigma(\tau^{-1}(T)) = \sigma(T) = T$$

亦知 $\sigma\tau^{-1} \in K$.

这两个子群是有区别的，一个保持集合 T 不动，一个保持 T 中每个元都不动. 若 T 只含一个元素，则 $H = K$. 若 $T = \{1, \cdots, n\}$，则

$$H = \{e\}, \qquad K = G.$$

任意群 G 都有两个极端子群 G 和 $\{e\}$，通常称为 G 的平凡子群.

习　题

1. 设非零复数在数的乘法之下构成的群为 G，用 i 代表纯虚数，证明

$$\{1, -1, \mathrm{i}, -\mathrm{i}\}$$

是 G 的一个子群.

2. 证明，所有形如

$$\begin{pmatrix} 1 & m & p \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}, m, n, p \in \mathbf{Z}$$

的矩阵的集合是实的 3 阶完全线性群的一个子群.

3. 在复的 2 阶完全线性群 G 中，矩阵

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad A = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix},$$

$$B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad C = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix},$$

$$-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad -A = \begin{pmatrix} -\mathrm{i} & 0 \\ 0 & \mathrm{i} \end{pmatrix},$$

$$-B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad -C = \begin{pmatrix} 0 & -\mathrm{i} \\ -\mathrm{i} & 0 \end{pmatrix},$$

构成 G 的一个子群.

4. 在四阶对称群 S_4 中令 $T=\{1, 2\}$，求

$$H = \{\sigma \in G \mid \sigma(t) = t, t = 1, 2\},$$

$$K = \{\sigma \in G \mid \sigma(T) = T,\}.$$

5. 看一个实的四元函数

$$f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3 + x_4.$$

证明，所有使 f 不变的四阶置换 σ，即使

$$f(x_{\sigma(1)}, \cdots, x_{\sigma(4)}) = f(x_1, x_2, x_3, x_4)$$

的置换构成四阶对称群的一个子群.

6. 在 §1 例 4 给出的群 $(A, \circ)$ 中，令

$$B = \{f_{a,0} \mid a \in \mathbf{R}, a \neq 0\},$$

$$C = \{f_{1,b} \mid b \in \mathbf{R}\}.$$

问 B 是 A 的子群吗？C 是 A 的子群吗？进一步，证明，对任意 $f \in A$，均有 $g \in B$，$h \in C$ 使得

$$f = g \circ h.$$

7. 条件如上题，给出 $f_{1,1}$ 在 A 中生成的子群.

§3 循环群

上节讨论子群时已经看到，由一个元素生成的子群表达起来相当简单，运算规律相当明了.

进一步学习群论将会看到，这种由一个元素生成的群可以派生出很多复杂而有实际意义的群.

定义 1 群 G 称为**循环群**，如果有 $g \in G$ 使得 $G=\langle g\rangle$. 也有人称循环群为**巡回群**.

例如，复数乘法群 $G=\{1, -1, \mathrm{i}, -\mathrm{i}\}$ 中，$G=\langle \mathrm{i}\rangle$，故 G 为循环群.

又如，四阶对称群中，

$$e, \quad g = (1\ 2\ 3\ 4),$$

$$g^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad g^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

构成一个群，它是由 g 生成的.

再如，整数加法群 $\mathbf{Z}$，它是由 1 生成的，当然也是由 -1 生成的，故 $\mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$ 是个循环群.

命题 1　设 G 是个群，$g \in G$. 如果有不同的整数 r, k 使 $g^r = g^k$，则必有一个正整数 m 使得

(1) $g^m = e$;

(2) 对 $1 \leqslant i < j \leqslant m$ 时，$g^i \neq g^j$;

(3) 对任意整数 t，若 $g^t = e$，则 m 整除 t;

(4) $\langle g \rangle = \{e, g, g^2, \cdots, g^{m-1}\}$.

证明　不妨设 $r > k$. 由于 $g^r = g^k$，两端同乘 g^{-k} 可得 $g^{r-k} = e$. 这说明有正整数 t 使 $g^t = e$，从而集

$$M = \{t \in \mathbf{Z} \mid g^t = e, t > 0\}$$

非空. 它必有一个最小元，设为 m.

首先有 $g^m = e$.

其次，当 $1 \leqslant i < j \leqslant m$ 时，由 $0 < j - i < m$ 知

$$g^{j-i} \neq e, \qquad g^i \neq g^j.$$

再次，对任意 $t \in \mathbf{Z}$，若 $e = g^t$，作整数除法，设有 q, $l \in \mathbf{Z}$ 使

$$t = mq + l \quad 0 \leqslant l < m,$$

则

$$e = g^t = g^{mq} g^l = (g^m)^q g^l = g^l,$$

而 m 是 M 之最小元，故 $l \notin M$, $l = 0$，即 m 必整除 t.

最后，由于 $g^m = e$, $g^{m+1} = g$, $\cdots$. 由 g 生成的子群 $\langle g \rangle$ 只含 m 个不同的元素，即

$$\langle g \rangle = \{e, g, g^2, \cdots, g^{m-1}\}.$$

命题 2　设 G 是个群，$g \in G$. 如果对任意不同的整数 r, k

都有 $g^r \neq g^k$，则$\langle g \rangle$是个无限群.

实际上

$$\langle g \rangle = \{\cdots, g^{-1}, e, g, \cdots, g^n, \cdots\},$$

这种表达中，元素两两不同，$\langle g \rangle$含无穷多个元素.

命题 1 和命题 2 概括了循环群的所有情况，使我们对循环群的结构一目了然. 下面讨论循环群的一些简单性质.

命题 3 无限循环群 G 只有两个生成元.

若 $G = \langle g \rangle$，则显然 $G = \langle g^{-1} \rangle$. 假如 g^n 亦为生成元，则应有 $m \in \mathbf{Z}$ 使 $g = (g^n)^m = g^{nm}$，必有 $mn = 1$，n 为 1 或 -1.

命题 4 设 G 是 m 元循环群. 如果正整数 n 与 m 互素，则生成元 g 的 n 次幂 g^n 亦为 G 的生成元.

事实上，$g^n \in G$，$\langle g^n \rangle \leqslant \langle g \rangle$. 而 m，n 互素时必有整数 s，t 使

$$sm + tn = 1,$$

于是

$$g = g^{sm} \cdot g^{tn} = (g^m)^s (g^n)^t = (g^n)^t,$$

即 $g \in \langle g^n \rangle$，从而知$\langle g \rangle = \langle g^n \rangle$.

命题 5 循环群的子群仍为循环群，且无限循环群的非平凡子群仍为无限循环群.

证明 若 G 为有限循环群

$$G = \{e, g, \cdots, g^{n-1}\},$$

它的任一子群 H 可设为

$$H = \{e, g^i, \cdots, g^k\},$$

其中 i，…，k 是大于 0 而小于 n 的不同的整数. 设 l 是其中最小者.

可以断言，l 必整除每个 i，…，k. 作除法，应有整数 q，r 使

$$i = ql + r, \quad 0 \leqslant r < l.$$

由于 $g^i \in H$, $g^l \in H$, 故 $g^{-l} \in H$, 进而

$$g^r = g^{i-ql} = g^i(g^{-l})^q \in H.$$

但 l 有最小性, 故 $r=0$, l 整除 i. 同理 l 整除 k. 所以

$$i = ql, \cdots, k = lm,$$

$$H = \{e, (g^l)^q, \cdots, (g^l)^m\} \subseteq \langle g^l \rangle.$$

另一方面, $g^l \in H$, $\langle g^l \rangle \subseteq H$, 故 $H = \langle g^l \rangle$.

设 G 为无限循环群, H 是 G 的子群. 当 $H=\{e\}$ 时, H 当然是循环群; 当 $H \neq \{e\}$ 时, 如果 $G=\langle g \rangle$, $g^i \in H$, $i \neq 0$, 则 $g^{-i} \in H$, 从而集合

$$\{i \in \mathbf{Z} \mid g^i \in H, i > 0\}$$

非空. 设 m 为该集之最小元. 可以断言, 任意 $g^n \in H$ 时, n 能被 m 整除. 从而 $\langle g^m \rangle \supseteq H$. 而 $\langle g^m \rangle \subseteq H$ 是显然的, 故 $\langle g^m \rangle = H$.

由于对任意整数 $i \neq j$, 必有 $im \neq jm$,

$$(g^m)^i \neq (g^m)^j,$$

故 $\langle g^m \rangle$ 为无限循环群.

命题 6　设 $G=\langle g \rangle$ 是个 n 元循环群, 且 $n=st$, 其中 s 和 t 是正整数, 则 G 有而且只有一个含 t 个元素的子群.

证明　看 g^s 生成的子群 $\langle g^s \rangle$, 由于

$$e, g^s, \cdots, g^{s(t-1)}$$

两两不同, 且 $(g^s)^t = e$, 知

$$\langle g^s \rangle = \{e, g^s, \cdots, g^{s(t-1)}\}$$

是 t 元群.

如果 G 还有子群 K 也是 t 元群, K 也是循环群, 可设 $k=\langle g^r \rangle$, 它的元素为

$$e, g^r, \cdots, g^{r(t-1)}$$

且 $g^{rt}=e$. 据命题 1, n 整除 rt, 即 st 整除 rt, s 整除 r, 从而知 $\langle g^r \rangle \subseteq \langle g^s \rangle$. 但两个群 $\langle g^r \rangle$, $\langle g^s \rangle$ 都是 t 元群, 最后得 $\langle g^r \rangle = \langle g^s \rangle$.

习　题

1. 证明，在复数乘法之下

$$\left\{1,\ -\frac{1}{2}+\mathrm{i}\frac{1}{2}\sqrt{3},\ -\frac{1}{2}-\mathrm{i}\frac{1}{2}\sqrt{3}\right\}$$

是个循环群，其中 i 是纯虚数.

2. G 是个群但不是循环群，它含四个元素，请完成其乘法表

	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

3. 设 $G=\langle g\rangle$ 是无限循环群，i, j 是两正整数，$H=\langle g^i\rangle$，$K=\langle g^j\rangle$，d 是 i, j 的最大公因数，m 是 i, j 的最小公倍数. 那么

$$K\cap H=\langle g^m\rangle,\quad \langle K\cup H\rangle=\langle g^d\rangle.$$

§4　陪集与阶数

定义 1　群 G 的元素的个数称为 G 的**阶数**，当 G 的元素个数有限时，用 $|G|$ 代表 G 的元数. 对于群 G 的元素 a，如果有正整数 n 使得 $a^n=e$，且 n 为使此等式成立之最小正整数，则说 a 的阶数为 n；如果找不到这样的数，则说 a 是无限阶的.

元素的阶数也称为元素的**周期**.

例如，整数加法群 $\mathbf{Z}$ 中每个非零整数 m 的阶都是无限的.

又如，非零复数构成的乘法群中，-1 的周期为 2，$-\frac{1}{2}+$

$i\frac{1}{2}\sqrt{3}$的周期为 3，i 的周期为 4，一般地，$\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$的周期为 n.

例 1　设 G 是从 $\mathbf{Z}$ 到$\{1,\ -1\}$上的所有映射的集合，在 G 上定义运算 · 并称为乘法，对任意 $f,\ g\in G$

$$f\cdot g:\ \mathbf{Z}\to\{1,\ -1\},$$
$$f\cdot g:\ x\to f(x)g(x).$$

可断言$(G,\ \cdot)$是个群.

对任意 $f,\ g,\ h\in G$，由于对任意 $x\in\mathbf{Z}$ 有

$$((f\cdot g)\cdot h)(x)=(f(x)g(x))h(x),$$
$$(f\cdot(g\cdot h))(x)=f(x)(g(x)h(x)),$$

知$(f\cdot g)\cdot h=f\cdot(g\cdot h)$.

G 中元

$$i:\ x\to 1$$

是 G 的恒等元.

对任意 $f\in G$，

$$(f\cdot f)(x)=f(x)f(x)=1=i(x),$$

即 $f\cdot f=i$，f 是自己的逆元.

故 G 是个群，每个非恒等元的周期均为 2，而且 G 是个无限群.

定义 2　设 H 是群 G 的一个子群，H 在 G 中确定一个关系如下：

$$a\sim b \text{ 当而且仅当 } ab^{-1}\in H,$$

称 ~ 是 H 在 G 中确定的**右关系**.

命题 1　设 H 是 G 的子群，则 H 在 G 上确定的右关系 ~ 是个等价关系.

证明　对任意 $a\in G$，因 $aa^{-1}\in H$，故 $a\sim a$.

如果 $a,\ b\in G$ 且 $a\sim b$，即 $ab^{-1}\in H$，由于 H 是 G 的子群，

必有

$$(ab^{-1})^{-1} = ba^{-1} \in H.$$

从而 $b \sim a$.

如果 $a, b, c \in G$ 且 $a \sim b$, $b \sim c$, 即 $ab^{-1} \in H$, $bc^{-1} \in H$. 由于 H 是个群, 知

$$(ab^{-1})(bc^{-1}) = ac^{-1} \in H,$$

从而 $a \sim c$.

例 2 在整数加法群 $\mathbf{Z}$ 中, 子群 $\langle 7 \rangle$ 确定的右关系是

$$i \sim j \quad \text{当而且仅当} \ i - j \in \langle 7 \rangle,$$

而一个整数 k 属于 $\langle 7 \rangle$ 的充要条件是它能被 7 整除. 故 $i \sim j$ 的充要条件是它们用 7 除之的余数相同.

子群 H 还可以定义左关系. 一般说来, H 在 G 中确定的左、右关系不一定一致.

例 3 在 3 阶对称群 G 中有 6 个元素

$$e = (1), \qquad a = (1\ 2), \qquad b = (1\ 3),$$
$$c = (2\ 3), \qquad d = (1\ 2\ 3), \qquad f = (1\ 3\ 2),$$

看子群 $H = \{e, a\}$ 所确定的左右关系. 计算得

$$cd^{-1} = cf = a \in H,$$
$$d^{-1}c = fc = b \notin H.$$

可知两个关系不一样.

定义 3 对于群 G 的任意非空子集 A, B, 称子集

$$\{g \in G \mid g = ab, a \in A, b \in B\}$$

为 A 与 B 的乘积, 记为 AB.

当 A 为子群, $B = \{b\}$ 时, 记 $AB = Ab$ 并称 Ab 是 A 在 G 中的一个**右陪集**; 称 $bA = BA$ 为 A 在 G 中的一个**左陪集**.

例 4 看例 3 的 3 阶对称群 G 及其子群 $H = \{e, a\}$, 有

$$Hd = \{ed, ad\} = \{d, c\},$$
$$Hf = \{f, b\},$$

$$dH = \{d, b\},$$
$$fH = \{f, c\}.$$

命题 2　设 H 是 G 的子群，~ 是 H 在 G 中确定的右关系. 那么，元素 a 在等价关系 ~ 之下的等价类恰好是 H 的右陪集 Ha.

证明　元素 a 在 ~ 之下的等价类是

$$S = \{b \in G \mid b \sim a\}.$$

如果 $b \in S$，$b \sim a$，即 $ba^{-1} \in H$，由 $ba^{-1} = h \in H$ 可知 $b \in Ha$，故 $S \subseteq Ha$. 反之，若 $b \in Ha$，即有 $h \in H$ 使 $b = ha$，$ba^{-1} = h \in H$，$b \sim a$，可知 $b \in S$，又得 $Ha \subseteq S$. 所以，$S = Ha$.

推论　设 H 是群 G 的子群，$a, b \in G$，那么 $ab^{-1} \in H$ 的充要条件是 $Ha = Hb$.

事实上，$ab^{-1} \in H$ 当而且只当 $a \sim b$，当而且只当 a，b 在同一等价类中，当而且只当 $Ha = Hb$.

命题 3　如果 H 是 G 的有限子群，则子集 Ha 的元素个数等于 H 的阶数.

证明　在集合 H 和 Ha 之间建立一个双射即可. 定义

$$f: H \to Ha,$$
$$f: h \to ha.$$

任取 $g \in Ha$，设 $g = xa$，$x \in H$，则

$$g = xa = f(x),$$

这说明 f 是满的. 另一方面，若有 $h_1, h_2 \in H$ 使 $f(h_1) = f(h_2)$，即 $h_1 a = h_2 a$，由于群满足消去律，必得 $h_1 = h_2$，这说明 f 是单的.

定理 1（Lagrange 定理）　设 G 是个有限群，那么 G 的任意子群 H 的阶数一定整除 G 的阶数.

证明　H 决定的右关系是 G 上的一个等价关系，每个右陪集就是一个等价类，设 $a_1, \cdots, a_k$ 构成等价关系 ~ 之下的一个

完全集，则

$$G = H_{a_1} \cup \cdots \cup H_{a_k},$$

即 G 的元素分成 k 组，每元在且只在某中一组，且各组元素数相同，均为 $|H|$，故 $|G| = k|H|$.

推论 1 若 G 是个有限群，则 G 的每个元素 a 的阶数均能整除 $|G|$.

事实上，元素 a 的阶数为 m，则 $\langle a \rangle$ 为 m 元子群，m 必整除 $|G|$.

推论 2 若 G 是个有限群，$|G|$ 为素数，则 G 没有非平凡子群.

因为素数 $|G|$ 只有两个正因子，其子群的阶数只能是 1 或者是 $|G|$，其子群只有 $\{e\}$ 和 G 本身.

推论 3 设 G 是有限群，$|G|$ 是个素数，则 G 为循环群.

事实上，由于 $|G| > 1$，取 $a \neq e$，则 a 的阶数不为 1，而 $\langle a \rangle$ 的阶数要想除 $|G|$，只能有 $|\langle a \rangle| = |G|$，从而 $\langle a \rangle = G$.

命题 4 设 G 是个群，H、K 是 G 的有限子群. 若 $|H| = m$，$|K| = n$，$|H \cap K| = s$，子集 HK 有 t 个元素，则 $mn = st$.

证明 笛卡尔积 $H \times K$ 有 mn 个元素. 我们在 $H \times K$ 上建立等价关系. 对任意 (h_1, k_2)，$(h_2, k_2) \in H \times K$，规定

$$(h_1, k_1) \sim (h_2, k_2) \text{ 当且仅当 } h_1k_1 = h_2k_2.$$

其等价性是显然的. 而且 $H \times K$ 在 $\sim$ 之下有 t 个不交的等价类.

现在来计算任意元 $(h, k) \in H \times K$ 的等价类中元素的个数.

若 $(h_1, k_1) \in H \times K$，$(h, k) \sim (h_1, k_1)$，即 $hk = h_1k_1$ 则 $h^{-1}h_1 = kk_1^{-1} = a \in H \cap K$，此时 $h_1 = ha$，$k_1 = a^{-1}k$.

反之，若 $b \in H \cap K$，由于 $(hb)(b^{-1}k) = hk$，必有

$$(h, k) \sim (hb, b^{-1}k).$$

这说明，若 $H \cap K = \{a_1, \cdots, a_n\}$，则 (h, k) 在 $\sim$ 之下的等价类是

$$\{(h, k), (h_{a_2}, a_2^{-1}k), \cdots, (h_{a_s}, a_s^{-1}k\},$$

这里假定了 $a_1 = e$.

$H \times K$ 有 t 个不交等价类. 每个等价类都含 s 元素，故 $mn = st$.

还有两个重要的命题，它们的计算有限群子群的阶数时很有用.

命题 5　设 S 是一个有限集合，G 是 S 上所有双射变换构成的群的一个子群. 且对 $s \in S$.

$$H_s = \{\sigma \in G \mid \sigma(s) = s\},$$

$$O_s = \{t \in S \mid t = \sigma(s), \text{对某个 } \sigma \in G\},$$

则 H_s 是 G 的一个子群，$|G|/|H_s|$ 等于 O_s 的元数.

证明　本章 §2 例 5 已经证明了 H_s 是 G 的一个子群.

在 G 上定义关系，对任意 $\sigma, \tau \in G$

$$\sigma \sim \tau \quad \text{当而且仅当} \sigma(s) = \tau(s).$$

则这是个等价关系. $\sigma \sim \tau$ 的充要条件是 $\tau^{-1}\sigma(s) = s$，充要条件是 $\tau^{-1}\sigma \in H_s$，充要条件是 $\sigma \in \tau H_s$，故 ~ 之下等价类的个数等于 H_s 在 G 中左陪集的个数，O_s 的元数等于 $|G|/|H_s|$.

定理 2(Cauchy 定理)　设 G 是个有限群，p 是素数，p 整除 G 的阶数 n，则 G 必有周期为 p 的元素.

证明　看 p 个 G 作成的笛卡尔积中所有满足下面条件的元素所构成子集 S:

1. $(x_1, x_2, \cdots, x_p) \neq (e, e, \cdots, e)$;

2. $x_1x_2\cdots x_p = e$.

由于任取 $x_1, \cdots, x_{p-1} \in G$，令 $x_p = x_{p-1}^{-1}\cdots x_1^{-1}$，即得一个满足条件 2 的元，故满足 2 的元素有 n^{p-1} 个，S 的元数为 $n^{p-1} - 1$.

研究 S 上的变换

$$\sigma(x_1, x_2, \cdots, x_p) = (x_2, x_3, \cdots, x_p, x_1),$$

当 $x_1x_2\cdots x_p=e$ 时，必有 $x_2\cdots x_px_1=e$，σ 是有意义的. 因为 σ^p 是 S 上恒等变换，所以

$$G_1=\{I,\sigma,\cdots,\sigma^{p-1}\}$$

是个 p 元循环群.

对 S 及 G_1 由命题5知，对 S 的任意元 s，其对应的 O_s 的元数或为 p 或为1. 如果每个 O_s 的元数都是 p，则由 S 诸 O_s 之并知 p 整除 $n^{p-1}-1$，而 p 整除 n. 矛盾. 故必有 S 的元 a，O_s 只含一个元素 $a=(y_1,y_2,\cdots,y_p)$，故 $H_s=G_1$，于是有

$$\sigma(a)=a,\ (y_1,y_2,\cdots,y_p)=(y_2,\cdots,y_p,y_1),$$

从而有 $a=(y,y,\cdots,y)$，$y\in G$，且 $y\neq e$，$y^p=e$. y 的周期为 p.

例5 设 $n\geqslant 3$，在 n 次对称群 S_n 中，由置换

$$\sigma=\begin{pmatrix}1 & 2 & 3 & \cdots & n-1 & n\\ 1 & n & n-1 & \cdots & 3 & 2\end{pmatrix}$$

和轮换 $\tau=(1,2,\cdots,n)$ 生成的子群 D_n 称为**二面体群**. 证明 D_n 的阶数为 $2n$.

解 首先应注意到 $\sigma^2=1$，且 τ 的周期为 n.

进一步，由

$$\sigma\tau=\begin{pmatrix}1 & 2 & 3 & \cdots & n-1 & n\\ 1 & n & n-1 & \cdots & 3 & 2\end{pmatrix}(1\ \cdots\ n)$$

$$=\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ 1 & n-1 & n-2 & \cdots & 1\end{pmatrix},$$

$$\tau^{-1}\sigma=\begin{pmatrix}1 & 2 & \cdots & n-1 & n\\ n & 1 & \cdots & n-2 & n-1\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots & n\\ 1 & n & \cdots & 2\end{pmatrix}$$

$$=\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ n & n-1 & n-2 & \cdots & 1\end{pmatrix},$$

知 $\sigma\tau=\tau^{-1}\sigma$.

再看 S_n 的子集

$$H=\{\tau^i\sigma^j\mid i=0,1,\cdots,n-1;j=0,1\},$$

对任意 i, $l=0, 1, \cdots, n-1$, 由

$$\tau^i\sigma\cdot\tau^l = \tau^i(\sigma\tau)\tau^{l-1} = \tau^i\tau^{-1}\sigma\tau^{l-1} = \tau^{i-l}\sigma,$$

$$\tau^i\sigma\tau^l\sigma = \tau^{i-1}\sigma^2 = \tau^{i-l}\sigma^0$$

知 H 是乘法封闭的, 且 $\tau^0\sigma^0=1\in H$, 加之

$$(\tau^i\sigma)^{-1} = \sigma^{-1}\tau^{-i} = \sigma\tau^{-i} = \tau^i\sigma \in H,$$

可推知 H 是 G 的子群. 又 σ, $\tau\in H$, 且对任意子群 $K\leqslant G$, 若 σ, $\tau\in K$, 则对任意 i, $j\in\mathbf{Z}$ 都应有 σ^i, $\tau^j\in K$, 故 $H\leqslant K$.

所以, $\langle\sigma, \tau\rangle = H$.

任取 i, $l=0, 1, \cdots, n-1$ 及 j, $k=0, 1$, 如果

$$\tau^i\sigma^j = \tau^l\sigma^k,$$

不妨设 $i\geqslant l$, 则得 $\tau^{i-l}=\sigma^{k-j}$. 因 σ 周期为 2, σ^{k-j} 等于 σ 或等于 1. 若 $\sigma^{k-j}=1$, 则 $\sigma^k=\sigma^j$, $\tau^i=\tau^l$, 得 $k=j$, $l=i$; 若 $\sigma^{k-j}=\sigma=\tau^{i-l}$, 作用在数字 1 上, 得

$$\tau^{i-l}(1) = i-l+1 = \sigma(1) = 1.$$

矛盾. 故 H 有 $2n$ 个不同的元素. D_n 的阶为 $2n$.

习　题

1. 设 H 是群 G 的子群. 证明 $HH=H$.

2. 设 G 是个有限群, H 是其子群, 且 $|G|=2|H|$. 那么, 对任意 a, $b\in G$, 若 $a\notin H$, $b\notin H$ 则必有 $ab\in H$.

3. 设 G 是个有限群, H 是其子群, 且 $|G|=2|H|$. 那么 G 对 H 的每个右陪集一定是个左陪集.

4. 设 G 是个交换群, a, $b\in G$ 的阶数分别为 m, n. 那么, 当 m, n 互素时, 元素 ab 的阶为 mn.

5. 设 G 是个群, a, $b\in G$. 那么 ab 的阶数与 ba 的阶数相同.

6. 若群 G 只有一个 2 阶元 a. 那么,对任意 $x\in G$ 恒有 $xa=ax$.

7. 设 G 是个群，H 是其所有非平凡子群的交集．如果 $H\neq\{e\}$，则 H 的每个元都是有限阶的．

§5 共轭与群方程

在计算有限群的元数及其某些子群的元数时，还有一种有用的分类方法．

设 G 是个群，对给定的 $g\in G$，如果 x，$y\in G$ 使

$$xg = gx, \qquad yg = gy,$$

则 $(xy)g=xgy=g(xy)$，$gx^{-1}=x^{-1}g$，故

$$N_g = \{x \in G \mid xg = gx\}$$

是 G 的一个子群，通常称为 g 在 G 中的**中心化子**．

定义 1 设 G 是个群，在其上定义关系

$$a \sim b \text{ 当且仅当有 } x \in G \text{ 使 } b = xax^{-1},$$

则 $\sim$ 是个等价关系．当 $a\sim b$ 时说 a 与 b **共轭**，a 所在的等价类称为 a 的**共轭类**．

命题 1 设 G 是个有限群，$g\in G$，则 g 所在的共轭类 S_g 恰好含 $|G|/|N_g|$ 个元素．

证明 建立 G 到 S_g 的映射

$$f:\ a \to aga^{-1},$$

则可得 G 上的一个关系

$$b \simeq a \text{ 当而且仅当 } bgb^{-1} = aga^{-1},$$

显然，$\simeq$ 是 G 上的一个等价关系．$\simeq$ 将 G 分成不相交的等价类，不同的等价类对应的 g 的不同的共轭元，即 S_g 的元数等于商集 $G/\simeq$ 的元数．

现在看 $\simeq$ 之下的任意一个等价类的个数．对任意 $a\in G$，若 $b\simeq a$，即

$$aga^{-1} = bgb^{-1},$$

则$(a^{-1}b)g=g(a^{-1}b)$，即$a^{-1}b\in N_g$，$b\in aN_g$. 反之，若$b\in aN_g$，设$b=ax$，$x\in N_g$，则

$$bgb^{-1}=(ax)g(ax)^{-1}=a(xgx^{-1})a^{-1}=aga^{-1}.$$

所以$b\in aN_g$的充要条件是$b\simeq a$. 换言之，与a有$\simeq$等价关系的元素共$|N_g|$个.

故知，$G/\simeq$的元数为$|G|/|N_g|$，它也就是S_g的元数.

上节中，有限群G用它的一个子群H作陪集分类时，每个陪集都含$|H|$个元素. 而用共轭关系分类时，各等价类所含的元素个数可能不一般多.

例如，对任意$x\in G$，由$x^{-1}ex=e$，知恒等元e只与自己共轭，即$S_e=\{e\}$. 同样，中心Z的每个元都是自共轭的，交换群的每个元素构成一个共轭类.

例 1　在n阶对称群S_n中注意如下事实，若$\sigma\in S_n$是一个轮换，设

$$\sigma=(i\,j\cdots k),$$

则对任意$\tau\in S_n$，有

$$\tau\sigma\tau^{-1}=(\tau(i)\ \tau(j)\ \cdots\ \tau(k)).$$

容易看出S_4有五个不交的共轭类，即

$\{e\}$，

$\{(12),(13),(14),(23),(24),(34)\}$，

$\{(12),(34),(13),(24),(14),(23)\}$，

$\{(123),(124),(134),(234),$
$(132),(142),(143),(243)\}$，

$\{(1234),(1324),(1243),(1342),(1432),(1423)\}$.

定理 1（群方程）　设G是个有限群，Z是其中心，在每个至少含两个元素的共轭类中各取一个代表元，记为$x_1,\cdots,x_k$，则

$$|G|=|Z|+\sum_{i=1}^{k}|G|/|N_{x_i}|.$$

证明 G 可写成不交的共轭类的并集. 其中，每个中心元自成一类，而 x_i 所在共轭类共有 $|G|/|N_{x_i}|$ 个元素.

命题 2 设 G 是有限群，Z 是其中心，$|G|=p^n$，其中 p 是素数，n 是个正整数. 那么 $|Z|\neq 1$.

证明 G 是交换群时，$G=Z$，$|Z|=p^n>1$. 若 G 不是交换群，对任意 $x\notin Z$，N_x 是 G 的真子群，$|N_x|$ 整除 p^n，$|G|/|N_x|$ 也整除 p^n，于是知 p 整除

$$\sum_{i=1}^{k}|G|/|N_{x_i}|,$$

故由群方程知 p 整除 $|Z|$.

命题 3 设 G 是个有限群，$|G|=p^2$，其中 p 为素数，则 G 是交换群.

证明 据命题2，$|Z|$ 等于 p 或 p^2，若 $|Z|=p^2$，则 $Z=G$，G 为交换群.

若 $|Z|=p$，则 Z 必为循环群，设

$$Z=\{e, a, \cdots, a^{p-1}\},$$

由于 $|G|=p^2$，$Z\neq G$，必有 $b\in G$，$b\notin Z$. 于是由 $|\langle a, b\rangle|$ 整除 p^2 且 $|\langle a, b\rangle|\neq p$ 知

$$|\langle a, b\rangle|=p^2, \qquad \langle a, b\rangle=G.$$

再由 a 是中心元，容易看出群 $\langle a, b\rangle$ 的任意两个元素均为可换的，从而 $G=\langle a, b\rangle=Z$，矛盾.

设 G 是个群，H 是 G 的子群，不难看出

$$N=\{x\in G \mid xH=Hx\}$$

是 G 的子群.

定义 2 设 G 是个群，H 是 G 的子群，且对任意 $g\in G$，恒有 $gH=Hg$，则说 H 是 G 的**正规子群**或**不变子群**，通常记为

$H \lhd G$.

定理 2　设 H 是群 G 的一个子群，则下列条件等价：

1. H 是 G 的正规子群；

2. 对任意 $g \in G$，$h \in H$ 有 $ghg^{-1} \in H$；

3. 对任意 $g \in G$，恒有 $gHg^{-1} = H$.

证明　若条件 1 成立，那么对任意 $h \in H$，由 $gh \in Hg$ 知有 $h_1 \in H$ 使 $gh = h_1 g$，从而

$$h_1 = ghg^{-1} \in H,$$

即条件 2 必然成立.

若条件 2 成立，则显然有 $gHg^{-1} \subseteq H$，但又应有 $g^{-1}(gHg^{-1})g \subseteq g^{-1}Hg \subseteq H$，故 $H = g^{-1}Hg$，对任意 $g \in G$ 都成立，即满足条件 3.

最后，若满足条件 3，$gHg^{-1} = H$，可推出 $gH = Hg$.

显然，$\{e\}$ 和 G 是 G 的正规子群，G 的中心 Z 是 G 的正规子群.

命题 4　设 G 是个群，K 是其子群，N 是 G 的正规子群，则 $KN = NK$ 且 KN 也是 G 的子群.

证明　任取 $x \in KN$，$x = kh$，$k \in K$，$h \in N$，因 N 是 G 的正规子群，应有

$$x = kh \in kN = Nk \subseteq NK,$$

故知 $KN \subseteq NK$. 同理还有 $NK \subseteq KN$.

进一步，G 之恒等元 e 属于 K 亦属于 N，故 $e = ee \in KN$.

任取 $k \in K$，$h \in N$，必有

$$(kh^{-1)} = h^{-1}k^{-1} \in NK = KN.$$

对任意 k，$k_1 \in K$，h，$h_1 \in N$，有

$$(kh)(k_1h_1) = k(hk_1)h_1 \in kNKh_1 \subseteq kKNh_1 \subseteq KN.$$

所以 KN 还是 G 的子群.

习　题

1. 设 H 是有限群 G 的子群，且 $|G| = 2|H|$，则 H 是 G 的不变子群.

2. 设 G 是个群，对任意 $i \in I$，N_i 都是 G 的不变子群，证明 $\bigcap_{i \in I} N_i$ 也是 G 的不变子群.

3. 若 N、H 都是群 G 的不变子群，则 NH 也是 G 的不变子群.

4. 举例，K、H 是群 G 的子群，KH 不是 G 的子群.

5. 设 G 是有限群，p 是素数，p 整除 $|G|$，且

$$H = \{x \in G \mid x^p = e\}$$

恰好含 p 个元素，证明，H 是 G 的正规子群.

§6　商　群

设 N 是群$(G, \cdot)$的一个不变子群，那么 G 对 N 的每个左陪集 aN 等于其右陪集 Na，由 N 在 G 中导出的左等价关系与右等价关系一致，这个等价关系记为 $\sim$.

$\sim$ 作为集合 G 上的一个等价关系引起 G 的一个分类，我们得到商集

$$G/N = G/\sim = \{aN, bN, \cdots\}$$

它以 N 的陪集作元素.

定理 1　设 N 是群$(G, \cdot)$的一个不变子群，G/N 代表 G 对 N 的所有陪集构成的集合. 规定，任意 aN，$bN \in G/N$ 对应 G/N 的元素 abN，则得 G/N 的一个运算 $\circ$，即

$$aN \circ bN = (a \cdot b)N,$$

而且$(G/N, \circ)$是个群，称为$(G, \cdot)$对 N 的**商群**.

证明　首先要说明 abN 是由陪集 aN 和 bN 完全确定，与陪

集代表元选择无关，即所谓定义的合理性问题.

设 $a_1N=a_2N$，$b_1N=b_2N$，那么必有 N 的元素 u，v 使

$$a_1 = a_2u, \qquad b_1 = b_2v,$$

从而

$$a_1 \cdot b_1 = a_2 \cdot u \cdot b_2 \cdot v,$$

但 N 是 G 的不变子群 $Nb_2=b_2N$，又必有 $u' \in N$ 使 $ub_2=b_2u'$，故

$$a_1 \cdot b_1 = (a_2 \cdot b_2) \cdot u' \cdot v,$$

也就是

$$(a_1 \cdot b_1)N = (a_2 \cdot b_2)N.$$

所以，规定

$$aN \circ bN = (a \cdot b)N,$$

得 G/N 上的一个运算.

进一步，任取 aN，bN，$cN \in G/N$，有

$$(aN \circ bN) \circ cN = (a \cdot b)N \circ cN = ((a \cdot b) \cdot c)N,$$

而 G 对 $\cdot$ 满足结合律，故

$$(aN \circ bN) \circ cN = aN \circ (bN \circ cN).$$

即 G/N 对 $\circ$ 亦满足结合律.

设 e 是 G 的恒等元，看 $eN \in G/N$. 对任意 $aN \in G/N$，有

$$eN \circ aN = (e \cdot a)N = aN \circ eN,$$

这说明 eN 是 G/N 的恒等元.

任取 $aN \in G/N$，看 $a^{-1}N \in G/N$，有

$$aN \circ a^{-1}N = (a \cdot a^{-1})N = eN = a^{-1}N \circ aN.$$

这说明 G/N 的每个元都有逆元.

所以，$(G/N, \circ)$ 是个群.

例 1　在整数加群 $(\mathbf{Z}, +)$ 中，$\langle m \rangle$ 代表由正整数 m 生成的子群，即

$$\langle m \rangle = \{\cdots, -m, 0, m, 2m, \cdots\},$$

$\mathbf{Z}$ 关于$\langle m\rangle$的陪集是

$$0+\langle m\rangle,\ 1+\langle m\rangle,\ \cdots,\ m-1+\langle m\rangle,$$

因为0，1，…，$m-1$ 是完全集，故 G/N 有 m 个元素．把 $i+\langle m\rangle$简记为$[i]$，则

$$\mathbf{Z}/\langle m\rangle=\{[0],[1],\cdots,[m-1]\}.$$

当$0\leqslant i, j\leqslant m-1$，且 $i+j\leqslant m-1$ 时

$$\begin{aligned}[i]+[j]&=(i+\langle m\rangle)+(j+\langle m\rangle)\\&=(i+j)+\langle m\rangle\\&=[i+j],\end{aligned}$$

而若 $0\leqslant i, j\leqslant m-1$，但 $i+j\geqslant m$ 时，$i+j$ 所在的陪集与 $i+j-m$ 所在陪集相同，故

$$[i]+[j]=[i+j-m].$$

特别地，取 $m=4$，有

$$\mathbf{Z}/\langle 4\rangle=\{[0],[1],[2],[3]\},$$

其中

$$\begin{aligned}[0]&=\{\cdots,-4,0,4,8,\cdots\},\\ [1]&=\{\cdots,-3,1,5,9,\cdots\},\\ [2]&=\{\cdots,-2,2,6,10,\cdots\},\\ [3]&=\{\cdots,-1,3,7,11,\cdots\},\end{aligned}$$

乘法表

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

例 2 设 G 是所有实的二阶可逆矩阵作成的乘法群，N 是 G 中所有行列式等于 1 的矩阵作成的子群，则有 $N\lhd G$.

任取 $A\in G$，设 $|A|=\alpha$. 由于 A 可逆，$\alpha\neq 0$ 及矩阵

$$B=\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}\in G,$$

而且

$$|B^{-1}A|=|B|^{-1}|A|=\alpha^{-1}\alpha=1,$$

知 $B^{-1}A\in N$，$A\in BN$. 于是，集合

$$\left\{\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}N \,\middle|\, \alpha\in\mathbf{R},\ \alpha\neq 0\right\}$$

是 G 对 N 的陪集表示的一个完全集，可把商群写成

$$G/N=\left\{\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}N \,\middle|\, \alpha\in\mathbf{R},\ \alpha\neq 0\right\}$$

其运算是

$$\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}N\circ\begin{pmatrix}\beta & 0\\ 0 & 1\end{pmatrix}N=\begin{pmatrix}\alpha\beta & 0\\ 0 & 1\end{pmatrix}N.$$

一般说来，商群 G/N 是由 G 对原有运算派生出来的，G/N 会继承 G 的很多特性，例如 G 为交换群，则 G/N 为交换群，G 为有限群，则 G/N 必为有限群. 在第三章讲群的同态时，还要深入讨论. 同时，在那里也要深入研究怎样用 N 和 G/N 的性质来判断 G 的结构的问题.

在这里，先讲一些简单的性质.

命题 1　设 N 是 G 的不变子群，那么，商群 G/N 为交换群的充分必要条件是对任意 $a,b\in G$ 都有 $aba^{-1}b^{-1}\in N$.

证明　如果 G/N 是交换群，那么，对任意 $a,b\in G$ 应有

$$aN\circ bN=abN=baN=bN\circ aN,$$

即 ab 与 ba 在 N 的同一陪集中，也就是

$$(ab)(ba)^{-1}=aba^{-1}b^{-1}\in N.$$

反之，若对任意 $a,b\in G$，都有 $aba^{-1}b^{-1}\in N$，则

$$abN = baN,$$

故 G/N 可交换.

命题 2 设 G 是个交换群. 证明, G 的所有阶数有限的元素的集合 N 是 G 的一个不变子群, 且 G/N 的非恒等元的阶数都是无限的.

证明 G 中元 a 阶数有限的充要条件是有正整数 k 使 $a^k = e$. 首先有

$$e \in N.$$

对任意 $a, b \in N$, 设 $a^k = e$, $b^l = e$, 则

$$(ab)^{kl} = a^{kl}b^{kl} = e,$$

知 $ab \in N$.

若 $a \in N$, $a^k = e$, 则

$$a^{-k} = (a^{-1})^k = e, \ a^{-1} \in N.$$

所以 N 是 G 的子群, G 可换, $N \lhd G$.

任取 G/N 的一个元 xN, $x \in G$, 如果 xN 的阶数有限, 有 k 使 $(xN)^k = N$, 则

$$(xN)^k = x^kN = N.$$

$x^k \in N$, 又必有 l 使 $x^{kl} = e$, $x \in N$, 也就是 $xN = N$, xN 为 G/N 之恒等元.

命题 3 设 Z 是群 G 的中心, 且商群 G/Z 是循环群, 证明 G 本身是个交换群.

证明 设 G/Z 是由 aZ 生成的.

任取 $x, y \in G$, 在 G/Z 中应有整数 m, n 使得

$$xZ = (aZ)^m, \qquad yZ = (aZ)^n.$$

应有 $z, w \in Z$ 使

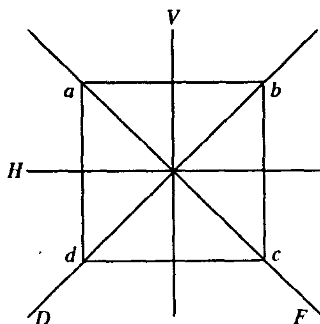
$$x = a^m z, \qquad y = a^n w,$$

于是

$$xy = a^m z a^n w = a^{m+n} zw = yx,$$

G 为交换群.

例 3　给出一个正方形如下:



用 $S=\{a, b, c, d\}$ 代表其顶点的集合. 现在来研究这个图形的运动(要保持刚体不变形). 只要掌握其顶点的运动情况, 则整个图形的运动情况也就清楚了.

看运动后与运动前之图形重合者. 它实质上是对顶点施以一次置换. 由于 S 上的置换只有 4! 个, 这类运动最多只有 24 个. 但实际上, 有些置换不可能表示正方形的运动, 例如

$$\begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix}$$

保持 a, b 不动, 让 c 变到 d, 而 d 变到 c, 是不可能实现的.

使正方形重合的运动有:

μ_1, 恒等置换;

μ_2, 绕 O 点顺时针转 90°;

μ_3, 绕 O 点顺时针转 180°;

μ_4, 绕 O 点顺时针转 270°;

μ_5, 以 H 为轴翻转 180°;

μ_6, 以 V 为轴翻转 180°;

μ_7, 以 D 为轴翻转 180°;

μ_8，以 F 为轴翻转 180°.

令 $G = \{\mu_1, \mu_2, \cdots, \mu_8\}$.

由于两个使该正方形重合的运动复合后仍使该正方形重合，恒等置换 μ_1 在 G 中，每个使该正方形重合的运动的逆变换也使该正方形重合，故 G 是 S_4 的一个子群.

G 的乘法表是

$\cdot$	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6	μ_7	μ_8
μ_1	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6	μ_7	μ_8
μ_2	μ_2	μ_3	μ_4	μ_1	μ_7	μ_8	μ_6	μ_5
μ_3	μ_3	μ_4	μ_1	μ_2	μ_6	μ_5	μ_8	μ_7
μ_4	μ_4	μ_1	μ_2	μ_3	μ_8	μ_7	μ_5	μ_6
μ_5	μ_5	μ_8	μ_6	μ_7	μ_1	μ_3	μ_4	μ_2
μ_6	μ_6	μ_7	μ_5	μ_8	μ_3	μ_1	μ_2	μ_4
μ_7	μ_7	μ_5	μ_8	μ_6	μ_2	μ_4	μ_1	μ_3
μ_8	μ_8	μ_6	μ_7	μ_5	μ_4	μ_2	μ_3	μ_1

设 $N = \{\mu_1, \mu_3\}$，则 N 为 G 的子群，且对任意 $\mu \in G$，恒有

$$\mu \cdot \mu_1 \cdot \mu^{-1} = \mu_1,$$

$$\mu \cdot \mu_3 \cdot \mu^{-1} = \mu_3.$$

故知 $N \lhd G$.

作陪集

$$[\mu_2] = \mu_2\{\mu_1, \mu_3\} = \{\mu_2, \mu_4\} = [\mu_4],$$

$$[\mu_5] = \mu_5\{\mu_1, \mu_3\} = \{\mu_5, \mu_6\} = [\mu_6],$$

$$[\mu_7] = \mu_7\{\mu_1, \mu_3\} = \{\mu_7, \mu_8\} = [\mu_8],$$

故

$$G/N = \{[\mu_1], [\mu_2], [\mu_5], [\mu_8]\}.$$

乘法表是

	$[\mu_1]$	$[\mu_2]$	$[\mu_5]$	$[\mu_7]$
$[\mu_1]$	$[\mu_1]$	$[\mu_2]$	$[\mu_5]$	$[\mu_7]$
$[\mu_2]$	$[\mu_2]$	$[\mu_1]$	$[\mu_7]$	$[\mu_5]$
$[\mu_5]$	$[\mu_5]$	$[\mu_7]$	$[\mu_1]$	$[\mu_2]$
$[\mu_7]$	$[\mu_7]$	$[\mu_5]$	$[\mu_2]$	$[\mu_1]$

习　题

1. 设 H 是 G 的子群. 在 G 对 H 的左关系下的商集 $G/\sim$ 中，规定，任意 aH，bH 对应 abH. 要此规定合理，H 必须是 G 的不变子群.

2. 给出对称群 S_3 的所有不变子群及相应的商群.

3. 证明

$$G = \{2^m 5^n \mid m, n \in \mathbf{Z}\}$$
$$N = \{2^m \mid m \in \mathbf{Z}\}$$

都是非零实数乘法群的子群，$N \lhd G$，并给出商群 G/N 的结构.

第三章 群同态

这一章处理群与群之间代数结构相似的问题.

学习线性代数时知道，同一个数域 F 上两个向量空间 V, U 的具体对象（向量）可能来自不同的背景，但只要它们的维数相同，就必然有相同的代数运算规律，研究起来非常方便. 这就是空间的“同构”.

对于群，我们采取同样的方法. “同构”实际上反映两个群的结构从代数观点看是完全相同的. 把这个要求放宽到某种意义上的相似，就是本章要讨论的“同态”.

§1 Caylay 定理

定义 1 设$(G, \cdot)$是个群，$(H, \circ)$也是个群. 如果有双射f: $G \to H$ 使得对任意 a, $b \in G$ 都有

$$f(a \cdot b) = f(a) \circ f(b),$$

则说群$(G, \cdot)$同构于群$(H, \circ)$，记为 $G \cong H$，并说f是 G 到 H 的一个**同构映射**.

例 1 看整数加群 $\mathbf{Z}$ 和所有偶数构成的子群 E. 规定，对任意 $m \in \mathbf{Z}$,

$$f(m) = 2m,$$

则 F 是个双射，且对每对 m, $n \in \mathbf{Z}$，有

$$f(m+n) = 2(m+n) = f(m) + f(n),$$

故$(\mathbf{Z}, +)$同构于$(E, +)$.

例 2 用 $\mathbf{R}^{+}$代表所有正实数的集合，它在数的乘法 · 之

下构成群，用$(\mathbf{R}, +)$表示实数加法群. 规定，对任意 $x \in \mathbf{R}^+$，

$$f(x) = \lg x,$$

则f是 $\mathbf{R}^+$ 到 $\mathbf{R}$ 的映射，是单的. 而且任取 $y \in \mathbf{R}$，令 $x = 10^y$，则

$$\lg x = \lg 10^y = y = f(x),$$

这说明f是满射.

进一步，对任意 $a, b \in \mathbf{R}^+$，

$$f(a \cdot b) = \lg(a \cdot b) = \lg a + \lg b = f(a) + f(b),$$

故，f是$(\mathbf{R}^+, \cdot)$到$(\mathbf{R}, +)$的一个同构映射.

我们已经知道，任意一个非空集合 A 上的所有双射变换(或可逆变换)在变换乘法(变换复合)之下构成一个群 $I(A)$.

群 G 上的双射变换f是 G 到 G 的同构映射时简称为 G 上**自同构**.

命题 1　设 G 是个群，则 G 的所有自同构构成$I(G)$的一个子群. 记为 $\mathrm{Aut}(G)$.

事实上，G 上恒等映射 i_G 是 G 的自同构，即 $i_G \in \mathrm{Aut}(G)$.

若$f, g \in \mathrm{Aut}(G)$，则$f \cdot g$ 仍为 G 上自同构，即

$$f \cdot g \in \mathrm{Aut}(G).$$

若$f \in \mathrm{Aut}(G)$，f是 G 上自同构. 看f的逆变换f^{-1}. 对任意 $x \in G$，若$f^{-1}(x) = y$，则必有$f(y) = x$. 所以，对每对 $a, b \in G$，设

$$f^{-1}(a) = c, \qquad f^{-1}(b) = d,$$

则应有 $a = f(c)$，$b = f(d)$，从而

$$\begin{aligned} f^{-1}(a \cdot b) &= f^{-1}(f(c) \cdot f(d)) = (f^{-1} \cdot f)(c \cdot d) \\ &= c \cdot d = f^{-1}(a) \cdot f^{-1}(b), \end{aligned}$$

故f^{-1}是自同构，$f^{-1} \in \mathrm{Aut}(G)$.

设 G 是个群，取定 $a \in G$，规定，对任意 $x \in G$，

$$\lambda_a: x \to ax,$$

称 λ_a 是 a 导出的 G 上**左乘变换**.

命题 2 群 G 上所有左乘变换的集合

$$L = \{\lambda_a \mid a \in G\}$$

是 $I(G)$ 的一子群.

证明 对于每个 $a \in G$, λ_a 一定是一个双射变换, 因若

$$\lambda_a(x) = \lambda_a(y), \quad ax = ay,$$

则必有 $x = y$. 同时, 对任意 $y \in G$, 恒有

$$y = a(a^{-1}y) = \lambda_a(a^{-1})y.$$

进一步, 设 e 是 G 的恒等元, 则

$$\lambda_e(x) = ex = x = i_G(x),$$

从而 $\lambda_e = i_G \in L$.

任取 λ_a, $\lambda_a \in L$ 及 $x \in G$, 有

$$(\lambda_a \cdot \lambda_b)(x) = \lambda_a \cdot (\lambda_b(x)) = a(bx) = \lambda_{ab}(x),$$

即

$$\lambda_a \cdot \lambda_b = \lambda_{ab} \in L.$$

对任意 $\lambda_a \in L$, 看 $\lambda_{a^{-1}}$, 对每个 $x \in G$, 有

$$(\lambda_{a^{-1}} \cdot \lambda_a)(x) = a^{-1}ax = x = i_G(x),$$

$$(\lambda_a \cdot \lambda_{a^{-1}})(x) = aa^{-1}x = x = i_G(x),$$

从而知 $\lambda_{a^{-1}} \in L$ 就是 λ_a 的逆.

命题 3 设 G 是个群, 则 G 同构于 G 上所有左乘变换构成的群 L.

证明 规定, 对任意 $a \in G$,

$$f: a \to \lambda_a.$$

首先, f 是单射. 因若

$$f(a) = f(b) = \lambda_a = \lambda_b,$$

则应有 $\lambda_a(e) = \lambda_b(e)$, 即 $ae = a = be = b$.

其次, f 是满射.

最后, 对任意 a, $b \in G$ 及 $x \in G$,

$$f(ab) = \lambda_{ab}, \quad \lambda_{ab}(x) = abx,$$

$$f(a)f(b) = \lambda_a\lambda_b, \quad \lambda_a\lambda_b(x) = abx,$$

故$f(ab) = f(a)f(b)$.

所以，f是G到L的同构映射.

把命题2和命题3结合起来，有

定理1(Caylay定理)　每个群G都同构于其上所有双射变换构成的群$I(G)$的一个子群.

推论　n阶有限群G必同构于n阶对称群S_n的一个子群.

实际上，若$G = \{a_1, a_2, \cdots, a_n\}$，$G$上可逆变换$\sigma$将$a_1, \cdots, a_n$变成$a_{i_1}, \cdots, a_{i_n}$，令$\sigma$对应

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}, \tag{1}$$

即得$I(G)$到S_n上一映射．如果记

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{i_1} & a_{i_2} & \cdots & a_{i_n} \end{pmatrix},$$

那么σ与置换(1)实质上只有记法不同，而运算的复合办法是一样的．所以，上边的对应就是一个群同构映射，$I(G)$同构于S_n.

历史上，首先出现的群是n阶对称群S_n和它的各种子群(通称为**置换群**)．现在，Caylay定理把抽象群与具体的置换群连起来，就使抽象群有了一个具体的表征.

记G是个群，$a \in G$，则a可导出G上的左乘变换λ_a，a^{-1}可导出G的右乘变换$\gamma_{a^{-1}}$，这两个变换都是自同构，它们的复合

$$\sigma_a = \lambda_a \cdot \gamma_{a^{-1}} = \gamma_{a^{-1}}\lambda_a$$

也是G的自同构，称为由a导出的内自同构．对任意$x \in G$，

$$\sigma_a(x) = (ax)a^{-1} = a(xa^{-1}).$$

命题 4 G 的所有内自同构的集合 $\mathrm{In}(G)$ 是 $\mathrm{Aut}(G)$ 的一个不变子群.

证明 首先，$\sigma_e = I_G \in \mathrm{In}(G)$.

其次，对任意 a，$b \in G$ 及 $x \in G$，

$$\begin{aligned}(\sigma_a \sigma_b)(x) &= a(bxb^{-1})a^{-1} \\ &= abx(ab)^{-1} = \sigma_{ab}(x),\end{aligned}$$

即 $\sigma_a \sigma_b = \sigma_{ab}$.

再次，对任意 $a \in G$，$\sigma_a \in \mathrm{In}(G)$，有

$$\sigma_a \sigma_{a^{-1}} = I_G.$$

这说明 $\sigma_{a^{-1}}$ 就是 σ_a 的逆，$(\sigma_a)^{-1} \in \mathrm{In}(G)$.

最后，对任意 $f \in \mathrm{Aut}(G)$ 及 $\sigma_a \in \mathrm{In}(G)$ 及每个 $x \in G$，有

$$\begin{aligned}f\sigma_a f^{-1}(x) &= f(af^{-1}(x)a^{-1}) \\ &= f(a)xf(a)^{-1},\end{aligned}$$

也就是 $f\sigma_a f^{-1} = \sigma_{f(a)} \in \mathrm{In}(G)$，$\mathrm{In}(G)$ 是 $\mathrm{Aut}(G)$ 的不变子群.

内自同构映射在群结构的研究中有重要作用，第二章引入的不变子群的概念可以叙述成，$N \lhd G$ 当而且仅当 $N \leqslant G$，且对任意 $\sigma_a \in \mathrm{In}(G)$，$h \in N$ 有

$$\sigma_a(h) \in N.$$

例题 用 D_n 代表 n 次二面体群(见第一章 §4 例题 5)，$n \geqslant 3$. 设群 G 由其两个元素 a，b 生成，且：

1. a 的周期为 n，b 的周期为 2，
2. $ba = a^{-1}b$.

证明，$D_n \cong G$.

解 一般说，G 的元素必形如

$$x = a^{m_1}b^{n_1}a^{m_2}b^{n_2}\cdots a^{m_k}b^{n_k};\ m_i,\ n_i \in \mathbf{Z},$$

但由条件 2，可将 x 化成形如 $a^m b^p$，m，$p \in \mathbf{N}$. 再由条件 1，可知 x 形如

$$a^m b^p;\ m = 0, 1, , n-1, p = 0, 1.$$

建立 D_n 到 G 的映射 φ,

$$\varphi:\ \tau^i\sigma^j \to a^i b^j;\quad i = 0, \cdots, n-1, j = 0, 1,$$

则 φ 是个满射，且 $\varphi(\tau) = a$, $\varphi(\sigma) = b$.

对任意 $\tau^i\sigma^j$, $\tau^k\sigma^l \in D_m$

$$\varphi(\tau^i\sigma^j \cdot \tau^k\sigma^l) = \varphi(\tau^{j-k}\sigma^{j+l}) = a^{i-k}b^{j+l}$$
$$= a^i b^j a^k b^l = \varphi(\tau^i\sigma^j)\varphi(\tau^k\sigma^l).$$

如果有 $\tau^i\sigma^j$, $\tau^k\sigma^l \in D_n$ 使

$$\varphi(\tau^i\sigma^j) = a^i b^j = a^k b^l = \varphi(\tau^k\sigma^l).$$

但 $b^i \neq b^l$，两端消去 b，可推出(注意 $b^2 = e$)

$$a^{i-k} = b,\quad i \geqslant k,$$

于是导致

$$a^{i+1-k} = a^{i-k}a = ba = a^{-1}b = a^{i-k-1},$$

即 $a^2 = e$，但 a 之周期为 $n \geqslant 3$，矛盾.

这说明 f 是 D_n 到 G 的一个同构映射.

习　题

1. 设 f 是群 G 到群 H 的一个同构映射，e 和 u 分别是 G 和 H 的恒等元，则

$$f(e) = u,$$

且对任意 $a \in G$, $f(a^{-1}) = f(a)^{-1}$.

2. 证明，所有的无限循环群都同构于整数加群 **Z**.

3. 设 Z 是群 G 的中心，证明 $g \in Z$ 的充分必要条件是对每个内自同构 σ_a 有 $\sigma_a(g) = g$.

4. 设 G 是个群，H 和 K 都是 G 的不变子群，且 $H \cap K = \{e\}$，那么，对任意 $x \in H$, $y \in K$ 恒有 $xy = yx$.

5. 称 $G = \{e, a, b, c\}$ 是**克莱因四元群**，其乘法表是

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

证明 Aut(G)同构于 3 次对称群 S_3.

6. S_4 的子群

$$H = \{(1), (12)(34), (13)(24), (14)(23)\}$$

和实可逆 2 阶矩阵乘法群的子群

$$G = \left\{\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}\right\}$$

同构，且它们的乘法表与上题之 G 相同.

7. 如果群 G 不是交换群，则必有 G 的一个交换的真子群 H，使 G 的中心 Z 真包含在 H 中.

§2 同 态

群的同构实际上是下面要讲的同态的一种特殊情形.

定义 1 设(G, ∘)是个群，(H, ·)也是个群，若 G 到 H 的映射 f 满足

$$f(a \circ b) = f(a) \cdot f(b), \quad a, b \in G,$$

则说 f 是 G 到 H 的一个**同态映射**，说 G 在 f 之下同态于 H.

所有的同构映射都是同态映射.

例 1 设 G 是所有实的 n 阶非奇异矩阵作成的乘法群，($\mathbf{R}^*$, ·)是所有非零实数的乘法群，规定

$$f(A) = |A|, \quad A \in G,$$

则对任意 A, $B \in G$ 有

$$f(AB) = |AB| = |A||B| = f(A) \cdot f(B),$$

故f是G到H的同态映射.

例2　设S_n是n阶对称群，$H=\{e, a\}$是个二元群，规定

$$f(A)=\begin{cases}e, & \text{如果 } A \text{ 为偶置换,}\\ a, & \text{如果 } A \text{ 为奇置换.}\end{cases}$$

由于任意A，$B\in S_n$，若A，B之奇偶性相同，则$f(A)=f(B)$，$f(A)\cdot f(B)=e=f(AB)$，若A，B之奇偶性不同，$f(A)$和$f(B)$中一个为e，一个为a，那么$f(A)\cdot f(B)=a=f(AB)$. 故f是同态映射.

例3　设G是个群，Aut(G)是其自同构群，σ_a代表G的元素a导出的内自同构，规定

$$f: a\rightarrow\sigma_a,$$

对任意a，$b\in G$及$x\in G$有

$$\begin{aligned}\sigma_{ab}(x)&=abx(ab)^{-1}=a(bxb^{-1})a^{-1}\\&=a\sigma_b(x)a^{-1}=(\sigma_a\cdot\sigma_b)(x),\end{aligned}$$

即$\sigma_{ab}=\sigma_a\cdot\sigma_b$，也就是

$$f(ab)=f(a)\cdot f(b),$$

这说明G同态于Aut(G).

注意，这个映射不一定是满的. 如果把Aut(G)换成内自同构群In(G)，就得到一个满的同态映射.

命题1　设f是群(G, $\circ$)到群(H, $\cdot$)的同态，e和u分别是G，H的恒等元，则

$$f(e)=u.$$

命题2　设f是群(G, $\cdot$)到群(H, $\circ$)的同态，则对每个$a\in G$有

$$f(a^{-1})=f(a)^{-1}.$$

这两个命题在上节已经作为习题留给读者，其实它们与f是否为双射没有关系.

定义2　设f是群G到群H的一个同态映射，$A\subseteq G$，$B\subseteq$

H，则

$$f(A) = \{f(a) \mid a \in A\} = \mathrm{Img}(A)$$

称为 A 在 f 下的**象**，$f(G)$ 也记为 $\mathrm{Img}(f)$.

$$f^{-1}(B) = \{a \in G \mid f(a) \in B\}$$

称为 B 在 f 下的**原象**.

当 $B=\{b\}$ 时，$f^{-1}(B)$ 可写成 $f^{-1}(b)$，注意不要与 f 为双射时 f 的逆映射 f^{-1} 混淆.

命题 3 设 f 是群 G 到群 H 的一个同态，u 是 H 的恒等元，那么 $f^{-1}(u)$ 是 G 的一个不变子群，记为 $\mathrm{Ker}(f)$.

证明 若 e 是 G 的恒等元，则 $f(e)=u$，即 $e \in f^{-1}(u)=\mathrm{Ker}(f)$.

若 $a,\ b \in \mathrm{Ker}(f)$，从而 $f(a)=u$，$f(b)=u$，则有

$$f(ab) = f(a)f(b) = uu = u,$$

即 $ab \in \mathrm{Ker}(f)$.

如果 $a \in \mathrm{Ker}(f)$，$f(a)=u$，那么 $f(a^{-1})=f(a)^{-1}=u$，从而知 $a^{-1} \in \mathrm{Ker}(f)$.

对任意 $g \in G$ 及 $a \in \mathrm{Ker}(f)$，有

$$f(gag^{-1}) = f(g)f(a)f(g)^{-1} = f(g)uf(g)^{-1} = u,$$

故知 $gag^{-1} \in \mathrm{Ker}(f)$.

所以 $\in \mathrm{Ker}(f)$ 是 G 的不变子群.

命题 4 若 f 是群 G 到群 H 的同态映射，g 是 H 到群 K 的同态映射，则 gf 是 G 到 K 的同态映射，且

$$\mathrm{Ker}(gf) = f^{-1}(\mathrm{Ker}(g)).$$

证明 gf 是同态映射一事读者可自行证明. 下面来证明这个 G 中子集等式.

任取 $a \in G$，如果 $a \in \mathrm{Ker}(gf)$，即 $(gf)(a)=e$，e 为 K 的恒等元. 由于

$$(gf)(a) = g(f(a)) = e,$$

即知$f(a)\in\mathrm{Ker}(g)$，进而$a\in f^{-1}(\mathrm{Ker}(g))$，也就是

$$\mathrm{Ker}(gf)\subseteq f^{-1}(\mathrm{Ker}(g)).$$

反之，若$a\in f^{-1}(\mathrm{Ker}(g))$，即$f(a)\in\mathrm{Ker}(g)$，也就是

$$g(f(a))=(gf)(a)=e,\quad a\in\mathrm{Ker}(gf).$$

因此$f^{-1}(\mathrm{Ker}(g))=\mathrm{Ker}(gf)$.

命题5　若f是群G到群H的同态映射，g是H到群K的同态映射，则$\mathrm{Img}(gf)=g(\mathrm{Img}(f))$.

证明　若$k\in K$，$k\in\mathrm{Img}(gf)$，即有$a\in G$使

$$k=(gf)(a)=g(f(a)),$$

而$f(a)\in\mathrm{Img}(f)$，故$k\in g(\mathrm{Img}(f))$.

反过来，若$k\in K$，$k\in g(\mathrm{Img}(f))$，则有$h\in\mathrm{Img}(f)$，$k=g(h)$，而$h\in\mathrm{Img}(f)$意味着有$a\in G$使$h=f(a)$，从而$k=g(h)=g(f(a))=gf(a)$，$k\in\mathrm{Img}(gf)$.

命题6　设f是群G到群H的同态映射. 如果A是G的子群，则$f(A)$是H的子群；如果B是H的子群，则$f^{-1}(B)$是G的子群. 当f是满射时，如果A是G的不变子群，则$f(A)$是H的不变子群；如果B是H的不变子群，则$f^{-1}(B)$是G的不变子群.

证明　若$A\leqslant G$，而e，u分别为G，H的恒等元，则$e\in A$，$f(e)=u\in f(A)$.

对任意x，$y\in f(A)$，必有a，$b\in A$使

$$x=f(a),\qquad y=f(b),$$

从而$xy=f(a)f(b)=g(ab)$，但A是子群，$ab\in A$，故知$xy\in f(A)$.

对每个$x\in f(A)$，设$a\in A$使$x=f(a)$，那么

$$x^{-1}=f(a)^{-1}=f(a^{-1}),$$

由于A是子群，$a^{-1}\in A$，故$x^{-1}\in f(A)$.

这说明$f(A)\leqslant H$.

若 $B \leqslant H$，则 $u \in B$，但 $f(e)=u$，故 $e \in f^{-1}(B)$.

对任意 a，$b \in f^{-1}(B)$，即

$$f(a) \in B, \qquad F(B) \in B.$$

由于 $B \leqslant H$，故

$$f(ab) = f(a)f(b) \in B,$$

也就是 $ab \in f^{-1}(B)$.

若 $a \in f^{-1}(B)$，$f(a) \in B$. $B \leqslant H$，故

$$f(a^{-1}) = f(a)^{-1} \in B.$$

即 $a^{-1} \in f^{-1}(B)$.

所以，$f^{-1}(B) \in G$.

当 f 是满射的时候，对任意 $h \in H$，必有 $a \in G$ 使 $h=f(a)$，于是，如果 $A \lhd G$，则必有

$$hf(A)h^{-1} = f(a)f(A)f(a^{-1}) \subseteq f(aAa^{-1}) = f(A),$$

即 $f(A) \lhd H$.

如果 $B \lhd H$，那么对任意 $a \in G$，及 $b \in f^{-1}(B)$，恒有

$$f(aba^{-1}) = f(a)f(b)f(a^{-1}) \in B,$$

即 $aba^{-1} \in f^{-1}(B)$，故 $f^{-1}(B) \lhd G$.

定义 2 设 N 是群 G 的不变子群，则

$$\gamma: g \to gN, \quad g \in G.$$

是群 G 到群 G/N 的满同态，称为**自然同态**.

定理 2（Sylow 定理） 设 G 是个有限群. $|G|=p^n m$，p 是素数，p 不整除 m. 那么，G 必有阶数为 p^n 的子群.

证明 对 $|G|$ 用数学归纳法. 当 $|G|=1$ 或 $n=0$ 时，命题显然正确.

现假定 $n \geqslant 1$，且对于阶数小于 $p^n m$ 的群，命题正确.

如果 G 有真子群 H，p^n 整除 $|H|$，由归纳法假定及 $|H|=p^n t$，t 整除 m，p 不能整除 t，可知必有 H 的子群，其阶数为 p^n，同时它也是 G 的子群. 命题得证.

故可设 p^n 不能整除 G 的任何一个真子群的阶数. 于是对于 G 的每一个真子群 H, p 必整除 $|G|/|H|$.

看群方程

$$|G| = |Z| + \sum_{i=1}^{k} |G| / |N_{x_i}|,$$

即知 p 整除 $|Z|$. 由第 2 章 §4 之定理 2 知, Z 必含一个周期为 p 的元素 z.

看 z 生成的子群 $\langle z\rangle$. 由于 z 含在 G 的中心 Z 里, $\langle z\rangle \subseteq Z$, $\langle z\rangle$ 必然是 G 的不变子群, 可得一商群 $H = G/\langle z\rangle$. 用 γ 代表 G 到 H 的自然同态映射.

由于 $|G| = p^n m$, $|\langle z\rangle| = p$, 据 Lagrange 定理, $|H| = p^{n-1}m$. 用归纳法假定, H 必含有一个阶数为 p^{n-1} 的子群 B.

据命题 6, $\gamma^{-1}(B)$ 是 G 的一个子群. 任取 B 中的一个元素 $b\langle z\rangle$, 它的原象恰好有 p 个元素, 即

$$b,\ bz,\ \cdots,\ bz^{p-1},$$

故 $|\gamma^{-1}(B)| = p^{n-1} \cdot p = p^n$, 归纳法完成.

这个定理是 Sylow p 群理论中的一个基础性定理, 对于研究有限群特别是有限单群的结构起重要作用.

命题 7　设 f 是群 G 到群 H 的同态映射, 那么, f 是单射的充分必要条件是

$$\mathrm{Ker}(f) = \{e\},$$

其中 e 为 G 之恒等元.

证明　若 f 为单射, $a \in \mathrm{Ker}(f)$, u 为 H 的恒等元, 则 $f(a) = u$, 但 $f(e) = u$, 由单射性知 $a = e$, 即 $\mathrm{Ker}(f) = \{e\}$.

反之, 若 $\mathrm{Ker}(f) = \{e\}$, 而有 $a, b \in G$ 使,

$$f(a) = f(b),$$

则 $f(a)f(b)^{-1} = f(ab^{-1}) = u$, 即 $ab^{-1} \in \mathrm{Ker}(f)$,

$$ab^{-1} = e, \qquad a = b,$$

f为单射.

命题 8 设f是群 G 到群 H 的同态映射，$A\leqslant G$, $B\leqslant H$, 则

$$f(f^{-1}(B)) = B\cap \mathrm{Img}(f),$$
$$f^{-1}(f(A)) = A\mathrm{Ker}(f).$$

证明 若 $b\in B\cap \mathrm{Img}(f)$，设 $a\in G$ 使得 $b=f(a)$，于是 $a\in f^{-1}(B)$，进而

$$b = f(a) \in f(f^{-1}(B)).$$

这说明 $B\cap \mathrm{Img}(f)\subseteq f(f^{-1}(B))$. 反方向的包含式是显然的.

由于 $A\leqslant G$, $\mathrm{Ker}(f)\lhd G$, 故

$$A\mathrm{Ker}(f) = \mathrm{Ker}(f)A \leqslant G.$$

若 $x\in \mathrm{Ker}(f)$，设 e, u 为 G, H 的恒等元，且

$$x = ak,\quad a\in A,\quad k\in \mathrm{Ker}(f),$$

则有

$$f(x) = f(a)f(k) = f(a)u = f(a) \in f(A).$$

于是 $x\in f^{-1}(f(A))$. 即 $A\mathrm{Ker}(f)\subseteq f^{-1}(f(A))$.

反之，若 $x\in f^{-1}(f(A))$，即$f(x)\in f(A)$，有 $a\in A$ 使$f(x)=f(a)$，故

$$u = f(a)^{-1}f(x) = f(a^{-1}x),\quad a^{-1}x\in \mathrm{Ker}(f),$$

从而 $x\in \mathrm{Ker}(f)$.

习 题

1. 设 G 是个群，$g\in G$. 规定

$$f:\ \mathbf{Z}\to G,$$
$$f:\ n\to g^n.$$

证明，f是整数加群 $\mathbf{Z}$ 到群 G 的群同态映射.

2. 条件如上题. 问，当 g 的周期为 3 时，$\mathrm{Ker}(f)$ 为何？当 g 之周期无限时，$\mathrm{Ker}(f)$ 的阶数如何？

3. 设($\mathbf{R}$, +)是实数加法群，($\mathbf{R}^*$, ·)是非零实数的乘

法群. 证明二者不同构.

4. 在实三维向量空间$(\mathbf{R}^3, +)$上令

$f: \mathbf{R}^3 \to \mathbf{R}^3$,

$f: (x, y, z) \to (x + 2y - z, 2x + y - z, x - y - 2z)$.

证明, f是群同态并求出 $\mathrm{Ker}(f)$.

5. $\mathbf{C}^*$代表非零复数作成的乘法群, $\mathbf{R}^+$代表正实数作成的乘法群, 令

$$f: \mathbf{C}^* \to \mathbf{R}^+,$$

$$f: a + ib \to \sqrt{a^2 + b^2},$$

证明, f是群同态并求出 $\mathrm{Ker}(f)$.

6. 求出加法群$(\mathbf{Z}, +)$到自己的所有的群同态映射.

7. 条件如本节例 3,

$$f: G \to \mathrm{Aut}(G),$$

$$f: a \to \sigma_a,$$

求出 $\mathrm{Ker}(f)$.

§3　同态基本定理

定理 1(同态基本定理)　设f是群 G 到群 H 的一个同态映射, 则群 $G/\mathrm{Ker}(f)$同构于群 $\mathrm{Img}(f)$.

证明　先来定义一个群 $G/\mathrm{Ker}(f)$到群 $\mathrm{Img}(f)$的映射. 规定, 任意 $a \in G$, $a\mathrm{Ker}(f) \in G/\mathrm{Ker}(f)$对应$f(a)$, 即

$$\varphi: G/\mathrm{Ker}(f) \to \mathrm{Img}(f),$$

$$\varphi: a\mathrm{Ker}(f) \to f(a).$$

由于上述规定是与代表元的选择相关联的, 需证明其合理性.

如果 $a_1\mathrm{Ker}(f) = a_2\mathrm{Ker}(f)$, 则有 $k \in \mathrm{Ker}(f)$使 $a_1 = a_2 k$, 从而

$$f(a_1) = f(a_2 k) = f(a_2)f(k) = f(a_2),$$

即 $\varphi(a_1\mathrm{Ker}(f))=\varphi(a_2\mathrm{Ker}(f))$. φ 的定义是合理的.

任取 $a\mathrm{Ker}(f)$, $b\mathrm{Ker}(f)\in G/\mathrm{Ker}(f)$. 由

$$\varphi(a\mathrm{Ker}(f)\cdot b\mathrm{Ker}(f))=\varphi(ab\mathrm{Ker}(f))=f(ab),$$
$$\varphi(a\mathrm{Ker}(f))=f(a),\quad \varphi(b\mathrm{Ker}(f))=f(b),$$

而 $f(ab)=f(a)f(b)$, 知 φ 是同态映射.

φ 是个满射.

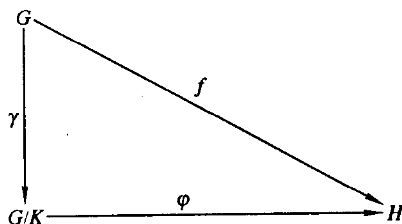
看 φ 的核 $\mathrm{Ker}(\varphi)$, 若 $a\in G$ 使

$$\varphi(a\mathrm{Ker}(f))=f(a)=u,$$

其中 u 为 H 的恒等元, 则 $a\in\mathrm{Ker}(f)$. $a\mathrm{Ker}(f)=\mathrm{Ker}(f)$ 是 $G/\mathrm{Ker}(f)$ 的恒等元, 故 φ 为单射.

所以, φ 是同构映射.

推论 设 f 是群 G 到群 H 的一个群同态映射, $K=\mathrm{Ker}(f)$, 则有 G/K 到 H 的群同态映射 φ 使下图形



可换.

证明 按定理证明中的定义,证 $\varphi\gamma$ 与 f 在 G 上作用效果相同.

任取 $a\in G$, 有

$$\varphi\gamma(a)=\varphi(\gamma(a))=\varphi(aK)=f(a),$$

这说明 $\varphi\gamma=f$.

例 1 用 $\mathbf{C}^*$ 代表所有非零复数构成的乘法群, $\mathbf{R}^+$ 代表所有正实数构成的乘法群. 任取非零复数 α, 可唯一地表成

$$\alpha=r(\cos\theta+\mathrm{i}\sin\theta),\quad 0\leqslant\theta<2\pi$$

形式. 其中 $r=|\alpha|$ 是 α 的模. 规定

$$f: \alpha \to r = |\alpha|, \quad \alpha \in \mathbf{C}^*,$$

则 f 是 $\mathbf{C}^*$ 到 $\mathbf{R}^+$ 的映射.

对任意 $\alpha, \beta \in \mathbf{C}^*$, 由于 $|\alpha\beta| = |\alpha||\beta|$, 即

$$f(\alpha\beta) = |\alpha\beta| = |\alpha||\beta| = f(\alpha)f(\beta),$$

知 f 是同态映射.

每个正实数 r 都是其本身的模 $r=f(r)$, f 是满射, $\mathrm{Img}(f) = \mathbf{R}^+$.

看 $\mathrm{Ker}(f)$, 任意 $a \in \mathbf{C}^*$, $f(\alpha) = |\alpha| = 1$ 的充要条件是 $\alpha = \cos\theta + \mathrm{i}\sin\theta$. 令

$$N = \mathrm{Ker}(f) = \{\alpha \in \mathbf{C}^* \mid \alpha = \cos\theta + \mathrm{i}\sin\theta\},$$

则 $\mathbf{C}^*/N$ 同构于 $\mathbf{R}^+$.

例题 1　求出使正方形重合的运动群(见第二章 §6 之例 3) G 的所有同态象.

解　由同态基本定理可知, 这等价于决定 G 的商群.

看 G 的不变子群. 由于 G 的阶数为 8, 它的子群的阶数只能是 1, 2, 4, 8.

对于平凡不变子群 $\{\mu_1\}$, G, 有

$$G/G \cong \{\mu_1\}, \qquad G/\{\mu_1\} \cong G.$$

现在来决定 G 的非平凡不变子群. G 有 4 阶子群, 例如 $\langle\mu_2\rangle$. 对于 G 的任意一个 4 阶子群 H 而言, 由于

$$|G| = 2|H|,$$

可知 H 一定是不变子群, 且 G/H 是 2 元群. 所有的 2 元群都是同构的, 它们同构于 $\mathbf{Z}/\langle 2\rangle$.

再看 G 的 2 阶子群. 2 阶子群必为循环群, 由周期为 2 的元素生成. G 中周期为 2 的元素是 μ_3, μ_5, μ_6, μ_7, μ_8. 显然, $\langle\mu_5\rangle$, $\langle\mu_6\rangle$, $\langle\mu_7\rangle$ 和 $\langle\mu_8\rangle$ 都不是不变子群. $\langle\mu_3\rangle \lhd G$.

看 $G/\langle\mu_3\rangle$ 的乘法表, 它的元素 $[\mu_2]$, $[\mu_5]$, $[\mu_7]$ 的周期

均为 2，它们生成的子群$\langle[\mu_2]\rangle$，$\langle[\mu_5]\rangle$和$\langle[\mu_7]\rangle$是 2 阶的，这些子群都是$G/\langle[\mu_3]\rangle$的不变子群. 而且

$$G/\langle[\mu_3]\rangle = \langle[\mu_2]\rangle\langle[\mu_5]\rangle.$$

且$\langle[\mu_2]\rangle\cap\langle[\mu_5]\rangle = \{[\mu_1]\}$.

实际上，看乘法表，我们知道$G/\langle\mu_3\rangle$是克莱因四元群.

总之，G 的同态象有

$$\langle[\mu_1]\rangle,\ \mathbf{Z}/\langle 2\rangle,\ \text{四元群},\ G.$$

命题 1 设 G 是个群，Z 是其中心，则 G/Z 同构于 $\mathrm{In}(G)$.

证明 沿用 §1 命题4 的符号，用 σ_a 代表 G 中元 a 导出的内自同构

$$\sigma_a: x \to axa^{-1},\quad x \in G.$$

看映射

$$f: G \to \mathrm{In}(G),$$
$$f: a \to \sigma_a.$$

由于 $\sigma_{ab} = \sigma_a\sigma_b$ 知 f 是群 G 到群 $\mathrm{In}(G)$ 的同态映射，而且是满的.

用 i_G 代表 G 的恒等映射，它是 $\mathrm{In}(G)$ 的恒等元. 若 $\sigma_a = f(a) = i_G$，即对任意 $x\in G$，有

$$\sigma_a(x) = axa^{-1} = x,$$

导致 $ax = xa$，$a\in Z$. 反之亦然. 故

$$\mathrm{Ker}(f) = Z,$$

由同态基本定理知 G/Z 同构于 $\mathrm{In}(G)$.

定理 2(Freshman 定理) 设 H 和 K 都是群 G 的不变子群，且 $K\lhd H$，那么 H/K 是 G/K 的不变子群，且群$(G/K)/(H/K)$同构于 G/H.

证明 用 γ 代表 G 到 G/K 的自然同态

$$\gamma(a) = aK,\quad a \in G.$$

由于 H 是 G 的不变子群，γ 是满同态，故 $\gamma(H)$必为 G/K 的不

变子群.

现断言 $\gamma(H)=H/K$. 事实上, 任取 $h\in H$, 则

$$\gamma(h) = hK \in H/K,$$

而对每个 $hK\in G/K$, $h\in K$ 均有

$$hK = \gamma(h) \in \gamma(H),$$

故 $\gamma(H)=H/K$.

进一步, G/K 到其商群 $(G/K)/(H/K)$ 有自然同态 φ

$$\varphi:\ aK \to aK\cdot H/K,\quad aK \in G/K.$$

由于 γ, φ 都是同态映射, 从而 $\varphi\gamma$ 是群 G 到 $(G/K)/(H/K)$ 的同态映射, 而且是满的.

计算 $\varphi\gamma$ 的核, 由 §2 命题 4, 知

$$\mathrm{Ker}(\varphi\gamma) = \gamma^{-1}(\mathrm{Ker}\varphi),$$

但 φ 是自然同态, 其核 $\mathrm{Ker}(\varphi)$ 就是 H/K, 所以

$$\mathrm{Ker}(\varphi\gamma) = \gamma^{-1}(H/K) = \gamma^{-1}(\gamma(H)) = HK = H.$$

由同态基本定理, 即知

$$G/K \cong (G/K)/(H/K).$$

定理 3　设 G 是个群, H 是 G 的子群, N 是 G 的不变子群, 则 $N\cap H$ 是 H 的不变子群, 且 $H/(N\cap K)$ 同构于 $(NH)/N$.

证明　显然, N 是 NH 的不变子群. 令

$$f:\ H \to NH/N,$$

$$f:\ x \to Nx,$$

容易验证 f 是满的群同态映射.

看 f 的核, 若 $x\in H\cap N$, 则

$$f(x) = Nx = N,$$

即 $x\in \mathrm{Ker}(f)$. 反之, 若 $x\in \mathrm{Ker}(f)$, $Nx=N$, 则 $x\in N\cap H$. 故知 $\mathrm{Ker}(f)=H\cap N$. 由同态基本定理推出, $H/(H\cap N)$ 同构于 $(NH)/N$.

习　　题

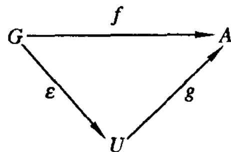
1. 证明每个无限循环群都同构于$(\mathbf{Z}, +)$，每个n阶循环群都同构于$\mathbf{Z}/\langle m\rangle$.

2. 设N是群G的不变子群，$|N| = m$，$|G| = mn$，且m和n互素. 证明N是G的唯一的一个m阶子群.

§4　可解群与组成列

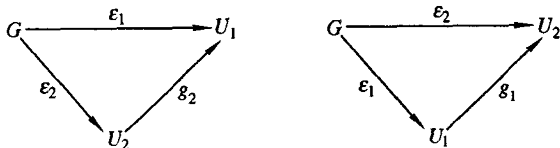
本节进一步研究如何用群G的不变子群N和商群G/N的性质来刻画G本身.

定义 1　设G是个群，U是个交换群，ε是G到U的满的群同态. 如果对任意交换群A及G到A的群同态f都有唯一的U到A的同态g使得右图可换，则说(U, ε)具有交换满同态泛性，简称有泛性.



命题 1　设(U_1, ε_1)和(U_2, ε_2)都对于G具有交换满同态泛性，则U_1和U_2同构.

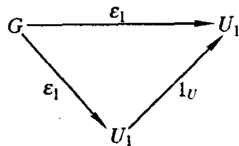
证明　由于泛性，我们有g_1，g_2使下两图



分别可换，即$g_1\varepsilon_1 = \varepsilon_2$，$g_2\varepsilon_2 = \varepsilon_1$，从而得

$$g_2g_1\varepsilon_1 = \varepsilon_1, \qquad g_1g_2\varepsilon_2 = \varepsilon_2,$$

但，对于(U_1, ε_1)已经有U上恒等映射1_U使右图可换. 由定义中的唯一性要求，应有$g_2g_1 = 1_{U_1}$，同理$g_1g_2 = 1_{U_2}$.



这说明 g_1 和 g_2 都是同构映射，U_1 同构于 U_2.

命题 2　任意群 G 都有交换群 U 和 G 到 U 的满同态使 (U, ε) 有泛性.

证明　G 中元素，$xyx^{-1}y^{-1}$ 称为 x、y 的**换位子**. 群 G 中所有换位子的集合生成的子群记为 G'. 实际上，G' 就是 G 中所有形如

$$(\#)\quad x_1y_1x_1^{-1}y_1^{-1}\cdots x_ny_nx_n^{-1}y_n^{-1},\quad n\in \mathbf{Z},\ x_i,\ y_i\in G$$

元素构成的集合.

首先 $eee^{-1}e^{-1}=e$ 为(#)形元素.

其次，两个(#)形元乘积仍保持原形式，亦为 G' 中元.

再次，任取(#)形元

$$(x_1y_1x_1^{-1}y_1^{-1}\cdots x_ny_nx_n^{-1}y_n^{-1})^{-1} = y_nx_ny_n^{-1}x_n^{-1}\cdots y_1x_1y_1^{-1}x_1^{-1}$$

也仍为(#)形元素.

最后，每个含所有换位子的子群必含全部(#)形元，故 G' 即 G 中全部(#)元的集合.

任取 $g\in G$ 及 G' 的一个元素，因

$$g(x_1y_1x_1^{-1}y_1^{-1}\cdots x_ny_nx_n^{-1}y_n^{-1})g^{-1}$$
$$=(gx_1g^{-1})(gy_1g^{-1})(gx_1g^{-1})^{-1}(gy_1g^{-1})^{-1}\cdots(gy_ng^{-1})^{-1}$$

仍在 G' 中，知 G' 是 G 的不变子群，称 G' 为 G 的**换位子子群**.

再来说明 G/G' 是交换的. 引用第二章 §6 命题 1 即可.

现在看来交换群 G/G' 及 G 到 G/G' 的自然同态映射 ε. 设 f: $G\to A$ 是 G 到交换群 A 的群同态映射. 对任意 x, $y\in G$, 由于 A 是可交换的，必有

$$f(x)f(y) = f(y)f(x),$$
$$f(xyx^{-1}y^{-1}) = u,$$

其中 u 是 A 的恒等元. 这说明 $xyx^{-1}y^{-1}\in \mathrm{Ker}(f)$，进而 $G'\leqslant \mathrm{Ker}(f)$.

我们定义 G/G' 到 A 的映射

$$g: xG' \to f(x),$$

需要证明合理性. 实际上，若 $xG' = yG'$，则

$$xy^{-1} \in G' \subseteq \mathrm{Ker}(f),$$

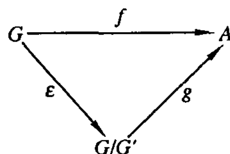
从而

$$f(xy^{-1}) = u, \qquad f(x) = f(y).$$

容易看出，g 是群同态映射，而且，对任意 $x \in G$，恒有

$$g\varepsilon(x) = g(xG') = f(x),$$

也就是右图形可换.



如果还有 $g_1: G/G' \to A$ 是群同态，使上图可换，则有

$$g\varepsilon = f = g_1\varepsilon,$$

而 ε 是满射，对每个 $xG' = \varepsilon(x)$ 有

$$g(xG') = g\varepsilon(x) = f(x) = g_1\varepsilon(x) = g_1(xG'),$$

也就是 $g = g_1$. 这说明满足要求的 g 是唯一的.

总之，$(G/G', \varepsilon)$ 对 G 具有泛性.

定义 2 设 G 是个群，令

$$G^{(0)} = G,\ G^{(1)} = G',\ G^{(2)} = (G^{(1)})',\ \cdots,$$
$$G^{(k+1)} = (G^{(k)})'.$$

如果有正整数 n 使 $G^{(n)} = \{e\}$，则说 G 是**可解的**.

命题 3 一个群 G 是可解的当而且仅当有 G 的子群

$$G = G_0 = G^{(0)} \geqslant G_1 \geqslant \cdots \geqslant G_m = \{e\},$$

使得 $G_{i+1} \lhd G_i$ 且 G_i/G_{i+1} 是交换群.

证明 如果 G 是可解的，有 n 使

$$G = G^{(0)} \geqslant G^{(1)} \geqslant \cdots \geqslant G^{(n)} = \{e\},$$

由于 $G^{(i+1)} = (G^{(i)})'$，故 $G^{(i+1)} \lhd G^{(i)}$，且 $G^{(i)}/G^{(i+1)}$ 是交换群。

反之，若有

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_m = \{e\}$$

且 $G_{(i+1)} \lhd G_{(i)}$，G_i/G_{i+1} 可交换，那么，G/G_1，可换，据第二章

§6之命题1，知 $G'\leqslant G_1$，由 G_1/G_2 可换又得 $(G_1)'\leqslant G_2$，从而

$$G^{(2)}=(G^{(1)})'\leqslant (G_1)'\leqslant G_2,$$

最后导出 $G^{(k)}\leqslant G_k$，对任意 k 都成立，故 $G^{(m)}=\{e\}$，G 是可解的.

定义3　若群 G 没有非平凡的不变子群，则说 G 是个**单群**. 若 G 的子群列

$$G=G_0\geqslant G_1\geqslant\cdots\geqslant G_m=\{e\}\tag{1}$$

中，对每个 i 都有 $G_{i+1}\lhd G_i$，且 G_i/G_{i+1} 为单群，则说(1)是 G 的一个**组成列**，诸 G_i/G_{i+1} 称为 G 的组成列(1)中的一个**列中商群**.

命题4　设 N 是 G 的不变子群. 那么，群 G/N 为单群的充分必要条件是：若 $H\lhd G$，$N\leqslant H$，且 $N\neq H$，必有 $H=G$.

证明　若有 $H\lhd G$，$N\lneqq H$，$H\neq G$，由§2命题6，在自然同态

$$\gamma:G\to G/N$$

之下，$\gamma(H)\neq N/N$，$\gamma(H)\neq G/N$，且 $\gamma(H)\lhd G/N$. 这说明 G/N 不是单群.

反之，若 G/N 不是单群，设有 $K\lhd G$，$N/N\neq K$ 且 $K\neq G/N$，则 $\gamma^{-1}(K)\neq N$，$\gamma^{-1}(K)$ 为 G 的不变子群，且 $G\neq\gamma^{-1}(K)$，否则导致 $\gamma(G)=\gamma\gamma^{-1}(K)=K$(据§2之命题8)，也就是 $G/N=K$. 矛盾.

定理1(Jordan-Holder 定理)　若有限群 G 有组成列

$$G=G_0\geqslant G_1\geqslant\cdots\geqslant G_m=\{e\},\tag{2}$$

$$G=H_0\geqslant H_1\geqslant\cdots\geqslant H_k=\{e\},\tag{3}$$

则 $m=k$，并且可在这两个组成列的列中商群集间建立一一对应，对应者是同构的.

证明　对 m 用数学归纳法.

若 $m=1$，则 G 为单群，没有非平凡的不变子群，故 $k=1$.

现假定命题对于有一个长度为 $m-1$ 的组成列的情形是对的. 如果 $G_1=H_1$，那么，由归纳法假设，命题对

$$G_1 \geqslant G_2 \geqslant \cdots \geqslant G_m = \{e\},$$
$$H_1 = G_1 \geqslant H_2 \geqslant \cdots \geqslant H_k = \{e\}$$

是对的，从而命题对于 G 是对的.

如果 $G_1 \neq H_1$，令 $K_2 = G_1 \cap H_1$. 由于 G/G_1 是单群，据命题 4，G 没有真包含 G_1 的不变子群，但 $G_1H_1 \geqslant G_1$，$G_1H_1 \lhd G$，且 $G_1H_1 \neq G_1$，故 $G_1H_1=G$，据 §3 之定理 3，应有

$$G/G_1 = G_1H_1/G_1 \cong H_1/(G_1 \cap H_1) = H_1/K_2,$$
$$G/H_1 = G_1H_1/H_1 \cong G_1/(G_1 \cap H_1) = G_1/K_2,$$

这说明 K_2 是 H_1 和 G_1 的不变子群，且 H_1/K_2 和 G_1/K_2 均为单群.

因为 K_2 是有限群，总可在 K_2 与 $\{e\}$ 之间填补得一组成列

$$K_2 \geqslant K_3 \geqslant \cdots \geqslant K_s = \{e\}.$$

研究 G_1 的组成列

$$G_1 \geqslant K_2 \geqslant \cdots \geqslant K_s = \{e\}, \tag{4}$$
$$G_1 \geqslant G_2 \geqslant \cdots \geqslant G_m = \{e\}, \tag{5}$$

由归纳法假定，得 $s-1=m-1$，即 $s=m$. 再看 H_1 的组成列

$$H_1 \geqslant K_2 \geqslant \cdots \geqslant K_s = \{e\},$$
$$H_1 \geqslant H_2 \geqslant \cdots \geqslant H_k = \{e\},$$

同样推知 $s=k$. 也就是 $m=k$.

再据归纳法假定，组成列(4)的列中商群与(5)的列中商群间有一一对应，对应者是同构的，进而组成

$$G \geqslant H_1 \geqslant K_2 \geqslant \cdots \geqslant K_m = \{e\} \tag{6}$$

与(3)

$$G \geqslant H_1 \geqslant H_2 \geqslant \cdots \geqslant H_m = \{e\}$$

列中商群间建立一一对应，对应者同构. 而组成列

$$G \geqslant G_1 \geqslant K_2 \geqslant \cdots \geqslant K_m = \{e\} \tag{7}$$

与组成列(2)

$$G \geqslant G_1 \geqslant G_2 \geqslant \cdots \geqslant G_m = \{e\}$$

有同样性质的对应.

注意(6)与(7)的前二项，我们已证得

$$G/G_1 \cong H_1/K_2, \qquad G/H_1 \cong G_1/K_2,$$

可知(6)和(7)的列中商群间可建立满足要求的对应，进而可在(2)与(3)间建立对应，归纳法完成.

命题 5　有限群 G 可解的充分必要条件是它的每个组成列的列中商群均为素数阶的循环群.

证明　设 G 是可解群，由命题 3，必有

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_m = \{e\}, \quad G_{i+1} \lhd G_i,$$

其中 G_i/G_{i+1} 是交换的. 由于这些群都是有限群，可以在 G_{i+1} 和 G_i 之间插入真子群

$$G_{i+1} \lhd H, \quad H \lhd G_i \quad G_{i+1} \neq H, \quad H \neq G_i$$

且到不能插入为止，即可得新排号的

$$G = G_0 \geqslant G_1 \geqslant \cdots \geqslant G_n = \{e\}$$

为 G 的一个组成列. 且 G_i/G_{i+1} 为交换群，单群. 但交换的有限单群之任意非恒等元必为该群的生成元，周期为素数，故 G_i/G_{i+1} 是素数阶的循环群.

反之是明显的.

习　题

1. 设 G 是 3 阶对称群，求出 G'.

2. 设 K 是 G 的不变子群，证明 K' 也是 G 的不变子群.

3. 设 H 是 G 的子群，$G' \subseteq H$. 证明，H 一定是 G 的不变子群.

4. 证明可解群的子群也是可解群.

§5 直 积

在平面解析几何学中，用直线 Ox，Oy 的笛卡尔积 $Ox \times Oy$ 来刻画一个平面；在线性代数学中讨论线性空间的直和，为把矩阵化成各种标准形式提供基础，这种由低级、简单的系统硬性组合出复杂新系统的方法在数学各分支中都是常见的.

设$(G, \cdot)$是群，$(H, \circ)$也是群. 考虑在集合 G 和 H 的笛卡尔积 $G \times H$ 上定义一个运算，它是由运算 $\cdot$ 和 $\circ$ 派生出来的，使 $G \times H$ 在此运算之下构成群.

定义 1 设$(G, \cdot)$和$(H, \circ)$是群，在 $G \times H$ 上规定，对任意(a, x)，$(b, y) \in G \times H$，对应 $G \times H$ 的元素$(a \cdot b, x \circ y)$，记为

$$(a, x)\#(b, y) = (a \cdot b, x \circ y),$$

则$(G \times H, \#)$是个群，称为是$(G, \cdot)$和$(H, \circ)$的**外直积**，简记为 $G \times H$.

由于运算#的实质是归结为在 G 和 H 上分别按 $\cdot$ 和 $\circ$ 运算，各行其事，$G \times H$ 在#之下构成群是非常容易验证的.

为了书写方便，今后把 G，H，$G \times H$ 的运算都写成 $\cdot$，有时都省略掉.

设 e 是 G 的单位元，u 是 H 的单位元，则(e, u)是 $G \times H$ 的单位元. 对任意 $a \in G$，$x \in H$，用 a^{-1}代表 a 在 G 中逆元，x^{-1}代表 x 在 H 中的逆元，则$(a, x)^{-1} = (a^{-1}, x^{-1})$.

若 G，H 都是交换群，则 $G \times H$ 也是交换群.

例题 1 如果 $G = \langle g \rangle$是 m 阶循环群，$H = \langle h \rangle$是 n 阶循环群，且 m，n 互素，则外直积 $G \times H$ 是 mn 阶循环群.

解 用 e，u 代表 G、H 的单位元. 看 $G \times H$ 的元素(g, h). 由于

$$(g, h)^{mn} = (g^{mn}, h^{mn}) = ((g^m)^n, (h^n)^m) = (e, u),$$

知(g, h)的周期不大于 mn.

另一方面，若有正整数 t，使$(g, h)^t = (e, u)$即 $g^t = e$，$h^t = u$，而 m 为 g 的周期，n 为 h 的周期，则必有 $m \mid t$，$n \mid t$，但 m，n 互素，故 $mn \mid t$. 这说明(g, h)的周期为 mn.

$G \times H$ 的元数为 mn，$\langle (g, h) \rangle$恰含 mn 个元素，故 $G \times H = \langle (g, h) \rangle$.

例题 2　设 p 是个素数，G 和 H 都是 p 阶群. 试决定外直积 $G \times H$ 的子群个数.

解　$G \times H$ 是个 p^2 阶群，由于 p 是素数，p^2 只有三个正因子，1，p，p^2，从而 $G \times H$ 的子群的阶数只能是 1，p，p^2. $G \times H$ 的 p^2 阶和 1 阶子群即 $G \times H$ 本身和$\{(e, u)\}$.

任取 $G \times H$ 的一个元素$(g, h) \neq (e, u)$，则

$$(g, h)^p = (g^p, h^p) = (e, u).$$

故$\langle (g, h) \rangle$是个 p 阶子群.

$G \times H$ 中共有 $p^2 - 1$ 个非恒等元，它们生成的子群含 $p - 1$ 个非恒等元，而任意两个不同的 p 阶子群交，仅含恒等元，故 $G \times H$ 的 p 阶子群有$(p^2 - 1)/(p - 1) = p + 1$ 个.

命题 1　设 G，H 是群，e，u 分别是它们的恒等元，令

$$G_1 = \{(g, h) \in G \times H \mid h = u\},$$

$$H_1 = \{(g, h) \in G \times H \mid g = e\},$$

则 G_1，H_1 是直积 $G \times H$ 的不变子群，且

$$G \times H = G_1 H_1 = H_1 G_1,$$

进一步，$G \times H$ 的任意元(g, h)写成

$$(g, h) = g'h', \quad g' \in G_1, h' \in H_1$$

时，表法唯一.

证明　很容易看出 $G_1 \lhd G \times H$，$H_1 \lhd G \times H$. 且对任意 $(g, h) \in G \times H$，有

$$(g, h) = (g, u)(e, h) = (e, h)(g, u),$$

故 $G \times H = G_1 H_1 = H_1 G_1$.

进一步，若对于 $(g, h) \in G \times H$，有 $g' \in G_1$，$h' \in H_1$ 使 $(g, h) = g'h'$，不妨设 $g' = (g_1, u)$，$h' = (e, h_1)$，则

$$g'h' = (g_1, u)(e, h_1) = (g_1, h_1) = (g, h),$$

从而导致

$$g_1 = g, h_1 = h, g' = (g, u), h' = (e, h).$$

这说明表法是唯一的.

定义 2 设 G 是个群，A 和 B 是 G 的子群，且

1. A 和 B 都是 G 的不变子群；
2. $G = AB$，即每个 $g \in G$ 均可写成 $g = ab$，$a \in A$，$b \in B$；
3. 对任意 $g \in G$，写成 $g = ab$，$a \in A$，$b \in B$ 时表法唯一.

则说 G 是其子群 A，B 的**内直积**.

例如，由命题 1 可知，任意两群 G，H 得到的外直积 $G \times H$ 恰好是其子群 G'和 H'的内直积.

又如，所有非奇异的二阶对角实矩阵的乘法群 G 有子群

$$A = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \middle| \alpha \in \mathbf{R} \right\},$$

$$\beta = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix} \middle| \beta \in \mathbf{R} \right\},$$

且 $A \lhd G$，$B \lhd G$，$G = AB$. 进一步可以证明表法唯一性. 故 G 是 A，B 的内直积.

命题 2 设 G 是个群，A 和 B 是它的不变子群. 那么，G 为 A 和 B 的内直积的充分必要条件是 $G = AB$ 且 G 的恒等元 e 写成 A 元与 B 元之积时表法唯一.

证明 因为 $A \lhd G$，$B \lhd G$，e 即为 G，A，B 各群的恒等元，且自然有一种表法 $e = ee$. 若 e 的表法唯一，即意味着只有上述这种表法.

此时，若对某个 $g\in G$ 有

$$g=ab=cd,\quad a,c\in A,\ b,d\in B,$$

则有 $(c^{-1}a)(bd^{-1})=e$，而 $c^{-1}a\in A$，$bd^{-1}\in B$，由于 e 表法唯一，应有 $c^{-1}a=e$，$bd^{-1}=e$，也就是 $c=a$，$d=b$. 这说明 g 的表法必唯一.

命题 3　设 G 是个群，A 和 B 是它的不变子群. 那么，G 为 A 和 B 的内直积的充分必要条件是 $G=AB$，且 $A\cap B=\{e\}$.

证明　若 $A\cap B=\{e\}$，而且有

$$e=ab,\ c\in A,\ b\in B,$$

则 $a=b^{-1}\in B$，从而 $a\in A\cap B$，$a=e$，进而 $b=e$. 这说明 e 的表法必唯一.

反之，若 e 的表法唯一. 任取 $x\in A\cap B$，则 $x^{-1}\in A\cap B$，故有 e 的一个表法

$$e=xx^{-1},\quad x\in A,\ x^{-1}\in B,$$

由唯一性推出 $x=e$. 即 $A\cap B=\{e\}$.

定理 1　设 G 是个群，A 和 B 是 G 的子群. 那么 G 为 A 和 B 的内直积的充分必要条件是

1. 对任意 $a\in A$，$b\in B$ 都有 $ab=ba$；

2. 对每个 $g\in G$，都有 $a\in A$，$b\in B$，使得 $g=ab$，而且表法唯一.

证明　若 G，A，B 满足条件 1 和 2，我们来证明 $A\lhd G$.

任取 $x\in A$，$g\in G$，必有 $a\in A$，$b\in B$ 使 $g=ab$，于是

$$gxg^{-1}=abxb^{-1}a^{-1}=axa^{-1}bb^{-1}=axa^{-1}\in A,$$

故 $A\lhd G$. 同理有 $B\lhd G$.

再利用条件 2，即知 G 为 A，B 的内直积.

反之，若 G 为 A，B 的内直积，那么，对任意 $a\in A$，$b\in B$，有

$$aba^{-1}b^{-1}=(aba^{-1})b^{-1}\in B,$$

$$aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in A,$$

从而 $aba^{-1}b^{-1} \in A \cap B = \{e\}$，也就是 $aba^{-1}b^{-1} = e$，$ab = ba$.

定理 2 若 G 是其子群 A，B 的内直积，则 $G \cong A \times B$.

证明 建立外直积 $A \times B$ 到群 G 的映射 φ，

$$\varphi: A \times B \rightarrow G = AB,$$

$$\varphi: (a, b) \rightarrow ab.$$

φ 是单射，因为若有 a，$c \in A$，b，$d \in B$ 使

$$\varphi((a, b)) = \varphi((c, d)),$$

即 $ab = cd$. 由内直积的表法唯一性可得 $a = c$ 且 $b = d$，即 $(a, b) = (c, d)$.

φ 是满射，因为任意 $g \in G$ 均可写成 $g = ab$，$a \in A$，$b \in B$，于是 $\varphi((a, b)) = ab = g$.

φ 还是群同态映射. 对任意 (a, b)，$(c, d) \in A \times B$ 有

$$\varphi((a, b)(c, d)) = \varphi(ac, bd) = (ac)(bd),$$

$$\varphi((a, b))\varphi((c, d)) = (ab)(cd),$$

但 A 的每个元与 B 的每个元均可换(定理 1)，故

$$(ab)(cd) = (ac)(bd).$$

对于任意有限个群的外直积和一个群是有限个不变子群的内直积的定义及相应的性质讨论，可以仿照以上两个群的直积的情形进行，没有原则上的变化，我们不予罗列. 现仅将定义给出.

定义 3 设 n 是个大于或等于 2 的整数. 对任意 n 个群 G_1，G_2，$\cdots$，G_n，在其笛卡尔积 $G_1 \times G_2 \times \cdots \times G_n$ 上规定运算

$$(g_1, g_2, \cdots, g_n)(h_1, h_2, \cdots, h_n) = (g_1h_1, \cdots, g_nh_n),$$

则 $G_1 \times \cdots \times G_n$ 成为群，称为 G_1，$\cdots$，G_n 的**外直积**.

设 G 是个群，A_1，$\cdots$，A_n 是 G 的子群，且：

1. A_1，$\cdots$，A_n 都是 G 的不变子群；
2. $G = A_1 \cdots A_n$，即每个 $g \in G$ 均可写成

$$g = a_1a_2\cdots a_n, \quad a_i \in A_i;$$

3. 对任意 $g \in G$，写成 $g = a_1\cdots a_n$，$a_i \in A_i$ 时表法唯一.

则说 G 是 A_1，…，A_n 的内直积.

读者可自行将本节之命题 1，2，3 和定理 1，2 推广到 n 个群的情形.

例题 3　若 G 是其子群 A_1，A_2，…，A_n 的内直积，则

$$G/A_1 \cong A_2\cdots A_n.$$

解　对任意 $g \in G$，恒有 $a_i \in A$，$i = 1$，…，n 使

$$g = a_1\cdots a_n,$$

且表法唯一，也就是说诸 a_i 由 g 唯一确定. 现规定

$$f: G \to A_2\cdots A_n,$$

$$f: g \to a_2\cdots a_n,$$

来证明 f 是群同态映射.

若 g，$h \in G$，且

$$g = a_1\cdots a_n, \quad h = b_1\cdots b_n, \quad a_i, b_i \in A_i,$$

那么，由于 G 是 A_1，…，A_n 的内直积，A_i 元与 A_j 元可换，故

$$gh = (a_1b_1)\cdots(a_nb_n).$$

再由表法唯一及 f 的定义，知

$$\begin{aligned} f(gh) &= (a_2b_2)\cdots(a_nb_n) \\ &= (a_2\cdots a_n)(b_2\cdots b_n) \\ &= f(g)f(h). \end{aligned}$$

对任意 $x \in A_2\cdots A_n$，设 $x = d_2\cdots d_n$，$d_i \in A_i$，那么

$$f(ed_2\cdots d_n) = d_2\cdots d_n = x.$$

这说明 f 是满的.

最后，计算 $\mathrm{Ker}(f)$.

若 $g = a_1a_2\cdots a_n$ 使 $f(g) = e$，即 $a_2\cdots a_n = e$，从而

$$g = a_1 \in A.$$

反之，若 $g \in A_i$，则 $g = ge \cdots e$ 即为其唯一表示，故

$$f(g) = e \cdots e = e, \ g \in \mathrm{Ker}(f).$$

所以，$\mathrm{Ker}(f) = A_1$. 由同态基本定理，有

$$G/A_1 \cong A_2 \cdots A_n.$$

现在，我们把外直积的概念推广到任意多个群的情形.

设 I 是个非空指标集，对任意 $i \in I$，有一个群 G_i，即有群族

$$\{G_i \mid i \in I\},$$

用 U 代表诸 G_i 之并集. 所有由 I 到 U 的映射构成的集合记为 F，它的子集

$$G = \{f \in F \mid f(i) \in G_i, \ i \in I\}$$

是个非空集. 规定，对任意 $f, g \in G$，

$$(f, g) \to f\#g,$$
$$[f\#g](i) = f(i)g(i).$$

$f\#g$ 是 I 到 U 的映射，且 $[f\#g](i) \in G_i$，因为 $f(i)$ 和 $g(i)$ 都是群 G_i 的元素，它们在 G_i 中的乘积仍为 G_i 中元素，故 $f\#g$ 是 G 中元.

任取 $f, g, h \in G$，来验证

$$(f\#g)\#h = f\#(g\#h).$$

因为这是映射的等式，只要验证它们对 I 中每个元 i 作用相同. 事实上，

$$[(f\#g)\#h](i) = (f\#g(i))h(i) = f(i)g(i)h(i),$$
$$[f\#(g\#h)](i) = f(i)g\#h(i) = f(i)(g(i)h(i)),$$

这是群 G_i 中元素的等式，由于 G_i 是个群，满足结合律，知#满足结合律.

用 e_i 代表 G_i 的恒等元，映射

$$\gamma(i) = e_i, \quad \text{对每个 } i \in I$$

是 G 的恒等元.

对任意$f\in G$，看映射

$$g(i)=f(i)^{-1},\quad 对每个 i\in I,$$

显然有$g\#f=f\#g=\gamma$，即g为f在G中的逆元.

总之，$(G,\#)$是个群，通常记为$\prod\limits_{i\in I}G_i$.

定义3　称$(G,\#)$为群族$\{G_i \mid i\in I\}$的直接积.

命题4　若I是n元集，则$\{G_i \mid i\in I\}$的直接积同构于它们的外直积.

证明　不妨设$I=\{1,2,\cdots,n\}$.

建立映射，令

$$\varphi:\prod_{i\in I}G_i\rightarrow G_1\times G_2\times\cdots\times G_n,$$

$$\varphi:f\rightarrow(f(1),f(2),\cdots,f(n)).$$

对任意$f,g\in\prod\limits_{i\in I}G_i$,

$$\begin{aligned}\varphi(f\#g)&=(f\#g(1),\cdots,f\#g(n))\\&=(f(1)g(1),\cdots,f(n)g(n))\\&=(f(1),\cdots,f(n))(g(1),\cdots,g(n))\\&=\varphi(f)\varphi(g).\end{aligned}$$

即φ是个同态映射.

任取$x_1\in G_1,\cdots,x_n\in G_n$，看$G$中元$f$(即$I$到$U$的映射)

$$f(1)=x_1,\cdots,f(n)=x_n,$$

必有

$$\varphi(f)=(f(1),\cdots,f(n))=(x_1,\cdots,x_n),$$

故，φ为满射.

如果$f,g\in G$而$\varphi(f)=\varphi(g)$，即

$$(f(1),\cdots,f(n))=(g(1),\cdots,g(n)),$$

从而

$$f(1)=g(1),\cdots,f(n)=g(n).$$

这说明f, g是相同的映射，$f=g$. 所以φ为单射.

总之，φ是个同构映射.

定义 4 在集族$\{G_i \mid i\in I\}$的直接积$\prod_{i\in I} G_i$中，所有只有限处不为恒等元的映射构成的集合记为$\sum_{i\in I} G_i$，称为族$\{G_i \mid i\in I\}$的**弱直积**.

对于I为有限集情形，$\prod_{i\in I} G_i = \sum_{i\in I} G_i$.

命题 5 对任意群族$\{G_i \mid i\in I\}$而言，其弱直积是直接积的一个不变子群.

证明 用e_i代替G_i的恒等元. 任取$f\in \sum_{i\in I} G_i$，设除有限处i_1, …, i_k外，

$$f(j) = e_j,$$

那么，对任意$g\in G$，当$j\neq i_1$, …, i_k时

$$g\#f\#g^{-1}(j) = g(j)f(j)g(j)^{-1} = g(j)e_j g(j)^{-1} = e_j,$$

这说明$g\#f\#g^{-1} \in \sum_{i\in I} G_i$.

习 题

1. 给出$\mathbf{Z}/\langle 2\rangle$, $\mathbf{Z}/\langle 3\rangle$的外直积的乘法表.

2. 给出$\mathbf{Z}/\langle 2\rangle\times\mathbf{Z}/\langle 2\rangle\times\mathbf{Z}\langle 2\rangle$的所有子群.

3. 设群G是其子群，A, B的内直积，且Z为G的中心，X是A的中心，Y是B的中心，则Z为X和Y的内直积.

4. 在非零有理数乘法群中，子群

$$G = \{2^m 5^n \mid m, n\in\mathbf{Z}\}$$

是其子群

$$N = \{2^m \mid m\in\mathbf{Z}\},$$

$$K = \{5^n \mid n\in\mathbf{Z}\}$$

的内直积.

5. 设 G, H 是群，则 $G\times H$ 的换位子群同构于 G 的换位子群与 H 的换位子群的外直积，即

$$(G\times H)'\cong G'\times H'.$$

第四章　环

前两章讨论的群是仅有一个二元运算的代数系统. 本章将要学习具有两个二元运算的代数系统. 近世代数学中常见的具有两个二元运算的代数系统有结合环，Lie 环，Jordan 环，格和 Boole 代数等. 其中结合环理论的背景最为广泛，研究的历史最长，已成为近世代数中最基本的内容之一.

§1　环的定义

定义 1　设集合 R 上有两个二元运算，一个叫加法，记为 $+$；一个叫乘法，记为 $\cdot$，且

1. $(R, +)$是个交换群；
2. 乘法 $\cdot$ 在 R 上是结合的；
3. 对任意 $a, b, c \in R$，都有

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{（左分配律）},$$
$$(b + c) \cdot a = b \cdot a + c \cdot a \quad \text{（右分配律）}.$$

则说$(R, +, \cdot)$是个**结合环**，简称环.

在不致引起混淆的情形下，也说 R 是个环，把 $a \cdot b$ 记成 ab. 环中运算，在无括号时，总是先乘后加.

例 1　整数集 $\mathbf{Z}$，有理数集 $\mathbf{Q}$，实数集 $\mathbf{R}$，复数集 $\mathbf{C}$ 和偶数集在数的加法，乘法下分别是个环.

例 2　设 F 为 $\mathbf{R}$ 上的所有变换的集合，即定义在$(-\infty, +\infty)$上的所有实函数的集合. 对任意$f, g \in F$，规定

$$f + g: x \to f(x) + g(x), \ x \in \mathbf{R},$$

$$f\cdot g: x\to f(x)\cdot g(x),\ x\in \mathbf{R},$$

则$(F, +, \cdot)$是环.

例 3　设 0 是加法群$(G, +)$的零元. 对任意 $a, b\in G$, 规定

$$a\cdot b = 0,$$

则$(G, +, \cdot)$是个环, 一般称为零乘环或零环.

例 4　四阶对称群 S_4 的子群

$$R = \{e, (12), (34), (12)(34)\}$$

是个交换群. 将 e, (12), (34), $(12)(34)$依次记为 e, a, b, c, 则其运算表为

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

用下一个运算表

·	0	a	b	c
0	0	0	0	0
a	0	a	0	a
b	0	b	0	b
c	0	c	0	c

得到 R 上另一个二元运算. 今证明$(R, +, \cdot)$是个环.

设 $x, y, z, u\in R$. 首先, 由 $u0=ub=0$ 知当 $z=0$ 或 b 时有

$$(xy)z = 0 = x(yz),$$

$$(x+y)z = 0 = xz+yz,$$

而由 $ua=uc=u$ 知当 $z=a$ 或 c 时, 有

$$(xy)z = xy = x(yz),$$
$$(x+y)z = x+y = xz+yz.$$

这说明 R 满足结合律和右分配律.

再则，只要 x, y, z 中有一个为 0，则必有

$$x(y+z) = xy+xz.$$

而当 $y=z$ 时，则有

$$x(y+y) = 0 = xy+xy.$$

看 x, y, z 均非零且 $y\neq z$ 的情形. 取 $y=b$，则 $z\neq b$，从而 $b+z\neq 0$, b. 于是知 z 与 $b+z$ 为 a 或 c，从而有

$$x(b+z) = x = xb+xz.$$

由群中加法运算的交换性知亦有

$$x(z+b) = xz+xb.$$

这是 y, z 中有一个为 b 的情形. 再看 y, z 均非 b 的情形. 注意 $y\neq z$ 且 y, z 又均非 0，知 y, z 中一为 a，另一为 c，从而 $y+z=b$，故有

$$x(y+z) = 0 = x+x = xy+xz.$$

于是知 R 亦满足左分配律. 故 R 为一环.

例 5 设 R 为一环，n 为一自然数，称

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}, \quad a_{ij}\in R$$

为 R 上矩阵. 对所有的 n 阶矩阵，像数域上矩阵那样定义加法与乘法，则形成一个环，称为 R 上 n 阶**全阵环**，记为 $M_n(R)$. 这是环理论中最重要的一类环.

例题 1 设$(G, +)$是个交换群，用 E 代表 G 的所有自同态(即 G 到 G 的同态映射)的集合. 规定，对任意 σ, $\tau\in E$, $x\in G$,

$$\sigma+\tau: x\to\sigma(x)+\tau(x),$$

$$\sigma \cdot \tau: x \to \sigma(\tau(x)),$$

则得到 E 上两个运算. 证明, $(E, +, \cdot)$ 是个环.

解　设 $\sigma, \tau \in E$. 由 $\sigma \cdot \tau$ 为 G 的自同态知 $\sigma \cdot \tau \in E$. 设 $x, y \in G$, 则

$$\begin{aligned}
&(\sigma + \tau)(x + y) \\
&= \sigma(x + y) + \tau(x + y) \\
&= \sigma(x) + \sigma(y) + \tau(x) + \tau(y) \\
&= \sigma(x) + \tau(x) + \sigma(y) + \tau(y) \\
&= (\sigma + \tau)(x) + (\sigma + \tau)(y),
\end{aligned}$$

易知 $\sigma + \tau$ 是 G 到 G 的映射, 而由上式知 $\sigma + \tau \in E$. 总之, $+$, $\cdot$ 是 E 上两个二元运算.

不难证明 $+$ 满足交换律和结合律, 零同态映射 0^*(即把 G 中元均映为 G 中零元的映射)是 E 的加法零元, 对任意 $\sigma \in E$,

$$-\sigma: x \to -\sigma(x), \quad x \in G$$

是 σ 在 E 中的负元. 于是, $(E, +)$ 是个交换群.

映射复合满足结合律. 今设 $\sigma, \tau, \rho \in E$, $x \in G$, 则有

$$\begin{aligned}
&[(\sigma + \tau) \cdot \rho](x) = (\sigma + \tau)[\rho(x)] \\
&= \sigma[\rho(x)] + \tau[\rho(x)] = (\sigma \cdot \rho)(x) + (\tau \cdot \rho)(x) \\
&= (\sigma \cdot \rho + \tau \cdot \rho)(x),
\end{aligned}$$

故有 $(\sigma + \tau) \cdot \rho = \sigma \cdot \rho + \tau \cdot \rho$, E 满足右分配律. 另一方面,

$$\begin{aligned}
&[\rho \cdot (\sigma + \tau)](x) = \rho[(\sigma + \tau)(x)] \\
&= \rho[\sigma(x) + \tau(x)] = \rho[\sigma(x)] + \rho[\tau(x)] \\
&= (\rho \cdot \sigma)(x) + (\rho \cdot \tau)(x) = (\rho \cdot \sigma + \rho \cdot \tau)(x),
\end{aligned}$$

故有 $\rho \cdot (\sigma + \tau) = \rho \cdot \sigma + \rho \cdot \tau$, E 满足左分配律. 于是, $(E, +, \cdot)$ 为一环.

E 称为 G 的自同态环. 应该注意, 证明左分配律时用到了映射 ρ 的同态性, 而证明右分配律时交未用到同态性.

例题 2　设 $G = \mathbf{Z}/\langle 2 \rangle = \{[0], [1]\}$, 用 F 代表所有 G 到

G 的映射的集合，$+$与$\cdot$的定义如例题 1. 那么，$(F, +, \cdot)$ 是个环吗？

解 令 σ 满足

$$\sigma([0]) = [1], \quad \sigma([1]) = [1],$$

则 $\sigma \in F$，但

$$[\sigma \cdot (\sigma + \sigma)]([1]) = [1],$$
$$(\sigma \cdot \sigma + \sigma \cdot \sigma)([1]) = [0],$$

$(F, +, \cdot)$不满足左分配律，非环.

看例题 1 的证明可知$(F, +, \cdot)$满足右分配律. 所以，在环的定义的公理中，两个分配律是独立的，需分别去验证.

命题 1 设$(R, +, \cdot)$是个环，0 是$(R, +)$的零元，$-a$ 代表$(R, +)$中 a 的负元，则对任意 $a, b, c \in R$，有

1. $0 \cdot a = a \cdot 0 = 0$;
2. $a \cdot (-b) = (-a) \cdot b = -a \cdot b$;
3. $(-a) \cdot (-b) = ab$;
4. $a \cdot (b - c) = a \cdot b - a \cdot c, \quad (a - b) \cdot c = a \cdot c - b \cdot c$.

证明 由

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$$

知 $0 \cdot a = 0$，类似地有 $a \cdot 0 = 0$. 由

$$a \cdot (-b) + a \cdot b = a \cdot [(-b) + b] = a \cdot 0 = 0$$

知 $a \cdot (-b) = -a \cdot b$，类似地有$(-a) \cdot b = -a \cdot b$. 剩余部分由 2 易得.

定义 2 设 R 是个环. 如果 R 的乘法有单位元 e(即恒等元)，则说 R 是个有单位元的环，或称有 1 环，称 e 为 R 的单位元(或恒等元). 若 $a \in R$，$a \neq 0$，而有 $b \neq 0$ 或 $c \neq 0$ 使 $ab = 0$ 或 $ca = 0$，则说 a 是 R 的一个**零因子**. 如果环 R 的乘法满足交换律，则说 R 是个交换环. 有 1 的无零因子的交换环为**整环**或**整区**.

例如，整数环、有理数环、实数环都是整环. 但偶数环不是整环，它没有乘法单位元.

命题2　设 R 是整区，则 R 的乘法满足消去律，即当 $a, b, c\in R$，$a\neq 0$ 时，$a\cdot b=a\cdot c$ 蕴含 $b=c$.

事实上，若 $a\cdot b=a\cdot c$，则有

$$0=a\cdot b-a\cdot c=a\cdot(b-c),$$

由于 R 无零因子，$a\neq 0$，知必有 $b-c=0$，即 $b=c$.

例题3　若环 R 中任意元 a 均满足

$$a\cdot a=a,$$

则 R 必为交换环.

解　任取 $a, b\in R$，则有

$$\begin{aligned}a+b&=(a+b)\cdot(a+b)\\&=a\cdot a+a\cdot b+b\cdot a+a\cdot a\\&=a+a\cdot b+b\cdot a+b,\end{aligned}$$

从而有

$$a\cdot b+b\cdot a=0. \tag{1}$$

用 a 代替(1)式中的 b，有

$$a+a=a\cdot a+a\cdot a=0,$$

即有 $a=-a$. 于是(1)变成

$$a\cdot b=-b\cdot a=b\cdot a,$$

知 R 为交换环.

由于环既是一个加法群又是一个有乘法的代数系统，所以，前两章中一些惯用的写法可直接使用. 例如，k 是自然数时，

$$a^k=aa\cdots a,\quad k\text{个}\ a\ \text{相乘},$$

$$ka=a+a+\cdots+a,\quad k\text{个}\ a\ \text{相加};$$

当 k 为负整数时，

$$ka=(-a)+(-a)+\cdots+(-a),\quad (-k)\text{个}(-a)\text{相加}.$$

命题3 设 R 是个有单位元 e 的环，则对任意 $n \in \mathbf{Z}$，$a \in R$，有

$$na = (ne)a.$$

证明 当 $n=0$ 时命题显然成立. 当 $n>0$ 时，

$$na = a + a + \cdots + a = ea + ea + \cdots + ea$$
$$= (e + \cdots + e)a = (ne)a.$$

当 $n<0$ 时，$m=-n>0$，且

$$na = m(-a) = (me)(-a)$$
$$= (-me)a = (ne)a,$$

其中 $(-me)=ne$ 是因为

$$me + ne = (e + \cdots + e) + [(-e) + \cdots + (-e)] = 0.$$

例6 设 R 为一环，x 为一文字，在集合

$$R[x] = \left\{ \sum_{i=0} a_i x^i \mid a_i \in R, \text{有限个 } a_i \neq 0 \right\}$$

规定它的两个元素

$$f(x) = a_0 x^0 + \cdots + a_n x^n, \quad a_n \neq 0 \tag{2}$$

$$g(x) = b_0 x^0 + \cdots + b_m x^m, \quad b_m \neq 0 \tag{3}$$

相等当而且仅当 $m=n$，且对应系数相等，即

$$a_0 = b_0, \cdots, a_n = b_n.$$

在 $R[x]$ 上仿实系数多项式定义加法与乘法，如

$$f(x)g(x)$$
$$= (a_0 b_0)x^0 + (a_0 b_1 + a_1 b_0)x^1 + \cdots + a_n b_m x^{m+n},$$

这里，当 R 不是交换环时，$f(x)g(x)$ 不一定等于 $g(x)f(x)$.

$R[x]$ 称为环 R 带文字 x 的**一元多项式环**. 环 $R[x]$ 带文字 y 的多项式环 $R[x][y]$，可记为 $R[x, y]$. 类似地，对于 n 个文字 $x_1, x_2, \cdots, x_n$ 有 R 上的多项式环

$$R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n],$$

称为 R 上 n 个文字多项式环，或 R 上 n **元多项式环**.

多项式理论是代数学的基石之一.

定义 3　设 R 是个有单位元 1 的环. R 的元 a 称为 R 的一个单位, 如果有 $b \in R$ 使

$$ab = ba = 1.$$

设 F 为一数域, 则 $M_n(F)$ 中的可逆矩阵就是单位. 从高等代数中知道, 如果 $A \in M_n(F)$, $A \neq 0$, 则不为零因子时必为单位.

但是, 此事实不能照搬到任意交换环的情形. 例如

$$T = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

为 $M_2(\mathbf{Z})$ 之一元、若有

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z})$$

使

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 2a & 2b \\ 2c & 2a \end{pmatrix},$$

则必有 $2a = 1$, $a \in \mathbf{Z}$. 这是不可能的. 故 T 不是 $M_2(\mathbf{Z})$ 的单位. 注意, 当 $A \neq 0$ 时, $AT = TA \neq 0$, 知 T 亦非零因子.

单位元是单位, 但单位不一定是单位元.

例题 4　设 R 为一环, $e \in R$ 是 R 的一个左单位元, 即满足条件:若 $x \in R$, 则 $ex = x$. 如果再设 e 是 R 中唯一的左单位元, 则 e 是 R 的单位元.

解　若有 $x \in R$ 使 $xe \neq x$, 则 $xe - x \neq 0$, 从而 $e + xe - x \neq e$. 但对任意 $y \in R$ 有

$$(e + xe - x)y = y + xy - xy = y,$$

即 $e + xe - x$ 为 R 之另一左单位元, 矛盾. 故对任意 $x \in R$ 恒有 $xe = ex = x$, 知 e 为 R 的单位元.

习　题

1. 用 E 代表偶数集，+是数的加法. 规定，对任意 $m, n \in E$，

$$m \cdot n = \frac{1}{2}mn.$$

证明，$(E, +, \circ)$是个环.

2. 设复数集 $A = \{a_1, \cdots, a_n\}$，$n > 1$，$+$，$\cdot$ 为数的加与乘. 证明，$(A, +, \cdot)$非环.

3. 环 R 为交换环的充分必要条件是，对任意 $a, b \in R$ 都有

$$a^2 - b^2 = (a + b)(a - b).$$

4. 设 F 为例 2 中的环，证明它是有零因子的环.

5. 设环 R 无零因子，$e \in R$，$e \neq 0$. 如果 $e \cdot e = e$，证明 e 是 R 的单位元.

6. 证明，有 1 交换环满足乘法消去律时必为整环.

7. 证明，任意一个恰含 5 个元素的环都是交换环.

8. 证明，有 1 环 R 是交换环的充分必要条件是对任意 $x, y \in R$ 恒有

$$(xy)^2 = x^2y^2.$$

§2　子环和理想

定义 1　设$(R, +, \cdot)$是个环，S 是 R 的一个非空子集. 如果 $+$ 和 $\cdot$ 也是 S 的运算，且$(S, +, \cdot)$也是个环，则说$(S, +, \cdot)$是$(R, +, \cdot)$的一个**子环**. 当所指运算不会混淆时，可简单地说 S 是 R 的子环.

例 1　整数环是有理数环的子环，二者都是实数环的子环.

例 2　用 C 代表 §1 例 2 之 F 中的所有连续函数的集合，

则 C 是 F 的子环.

例3　S 是 R 的子环时，$M_n(S)$ 亦为 $M_n(R)$ 的子环. $M_n(R)$ 中全部下三角矩阵，即

$$(a_{ij}) \in M_n(R), \quad i < j \text{时} \ a_{ij} = 0$$

形成 $M_n(R)$ 的一个子环. $M_n(R)$ 中所有形如

$$\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$$

的矩阵也作成 $M_n(R)$ 的一个子环，其中 A 是 m 方阵，$m \leqslant n$. $M_n(R)$ 中所有形如

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & 0 & \cdots & 0 \end{pmatrix}$$

的矩阵也作成 $M_n(R)$ 的一个子环.

命题1　设 R 是个环，S 为 R 的非空子集. 那么，S 是 R 的子环的充分必要条件是：

1. 对任意 a，$b \in S$，有 $a + b \in S$，
2. 对任意 $a \in S$，有 $-a \in S$，
3. 对任意 a，$b \in S$，有 $ab \in S$.

证明　如果 S 是 R 的子环，则 $(S, +)$ 是 $(R, +)$ 的子群，从而 S 满足 1 和 2. R 上的乘法也是 S 上的乘法，故 S 满足 3.

反过来，由 S 满足 1 和 2 知 $(S, +)$ 是 $(R, +)$ 的子群从而为一群. 由 1 和 3 知 $+$ 和 $\cdot$ 是 S 的运算，它们是从 R 的运算派生出来的，因而满足加法交换律、乘法结合律以及左和右分配律，于是 $(S, +)$ 是个交换群，$(S, +, \cdot)$ 为一环，S 为 R 的子环.

仿上可以证明.

命题2　设 R 是个环. 则 S 是 R 的子环的充分必要条件是：

1. $(S, +)$是$(R, +)$的子群;

2. 对任意 $a, b \in S$, 有 $ab \in S$.

例 4 在实数环 $\mathbf{R}$ 中, 所有形如

$$a + b\sqrt{2}, \quad a, b \in \mathbf{Z}$$

的数形成 $\mathbf{R}$ 的一个子环.

在复数环 $\mathbf{C}$ 中, 所有形如

$$a + b\mathrm{i}, \quad a, b \in \mathbf{Z}$$

的数形成 $\mathbf{C}$ 的一个子环, 称为 Gauss 整数环.

例 5 整数环 $\mathbf{Z}$ 的子集中, 所有偶数的集合 E 是 $\mathbf{Z}$ 的子环, 任意奇数的集合 S 都不是 $\mathbf{Z}$ 的子环:S 在减法之下不封闭, 例如 $a \in S$, 则

$$a - a = 0 \notin S.$$

例 6 例 2 的环 C 中, 子集

$$S = \{f \in C \mid f(2) = 0\}$$

是 C 的一个子环.

命题 4 设 S_a, $a \in I$ 都是环 R 的子环. 那么, 它们的交集

$$S = \bigcap_{a \in I} S_a$$

仍为 R 的子环.

证明 首先, 由 S_a 均为加群 R 的子群知 S 是加群 R 的子群. 设 $x, y \in S$, 则 $x, y \in S_a$, 对任意 $a \in I$. S_a 是子环, 从而有 $xy \in S_a$, $a \in I$. 于是有 $xy \in S$. 总之, S 是 R 的子环.

定义 2 设 R 是个环, $a \in R$. 令

$$A = \{S \mid S \text{ 是 } R \text{ 的子环}, a \in S\},$$

称 $\bigcap_{S \in A} S$ 为 R 的由 a **生成的子环**, 记为$\langle a \rangle$. 设 T 是 R 的一个非空子集, 可类似地定义 T **生成的子环**$\langle T \rangle$. 如果 T 是有限集 $\{a_1, \cdots, a_n\}$, 则记$\langle T \rangle = \langle a_1, \cdots, a_n \rangle$.

推论 $\langle T \rangle$是 R 的包含 T 的子环中的最小者.

证明　首先，$\langle T\rangle$本身为一包含 T 的子环. 其次，设 S_0 为 R 的一个包含 T 的子环，则

$$S_0 \in A = \{S \mid S\text{是}R\text{的子环},\ T \subseteq S\},$$

从而知

$$\langle T\rangle = \bigcap_{S\in A} S = S_0.$$

命题 5　设 R 是个环，$a\in R$. 那么，R 中所有形如

$$ma,\ ma + na^2,\ \cdots,\ m_1a + m_2a^2 + \cdots + m_ta^t,\ \cdots$$

的元(其中 $t, m, n, m_i \in \mathbf{Z}$, $t>0$)做成的集合 T 恰为$\langle a\rangle$.

证明　设 A 为定义 2 中那个子环族. 设 $x, y\in T$, 即 x, y 可以写成

$$x = m_1a + m_2a^2 + \cdots + m_ta^t,$$

$$y = n_1a + n_2a^2 + \cdots + n_ta^t,$$

其中某些 m_i 或 n_i 可能为 0. 于是有

$$x - y = (m_1 - n_1)a + \cdots + (m_t - n_t)a^t \in T,$$

$$xy = m_1n_1a^2 + \cdots + m_tn_ta^{2t} \in T.$$

若取 $t = m_1 = 1$，则有 $a\in T$，知 T 非空，从而为 R 的一个含 a 的子环，即 $T\in A$，于是有$\langle a\rangle = \bigcap_{S\in A} S \subseteq A$. 另一方面，若 $S\in A$，则 $a\in S$. 注意 S 为环，知所有形如 x 的元必在 S 中，从而有 $T\subseteq S$，$T\subseteq \bigcap_{S\in A} S = \langle a\rangle$. 总之，有 $T = \langle a\rangle$.

应用命题 5，可以知道整数环 $\mathbf{Z}$ 中元 8 生成的子环$\langle 8\rangle$中元具形

$$m8 + n64 + \cdots + k8^t = (m + 8n + \cdots + 8^{t-1}k)8,$$

故有

$$\langle 8\rangle = \{8m \mid m \in \mathbf{Z}\} = \{\cdots, -8, 0, 8, 16, \cdots\}.$$

仿命题 5，可以证明

命题 6　设 T 是环 R 的非空子集，则$\langle T\rangle$恰由下述形式的元组成：

$$a_1+\cdots+a_n+b_1c_1+\cdots+b_mc_m+\cdots+x_1\cdots x_t+\cdots+z_1\cdots z_l,$$

其中诸 a_i, b_j, ⋯, z_t 均为 T 中元或它们的负元.

如果命题 6 中的 $T=\{a,\ b\}$，则

$$a_1+\cdots+a_n=ka+lb,\quad k,\ l\in \mathbf{Z},$$

$$b_1c_1+\cdots+b_mc_m=sa^2+pab+qba+tb^2,\quad s,\ p,\ g,\ t\in \mathbf{Z}.$$

例题 1 求出整数环 $\mathbf{Z}$ 中 6 和 9 生成的子环 $\langle 6,\ 9\rangle$.

解 此子环含所有形如

$$k6+l9,\quad k,\ l\in \mathbf{Z} \qquad (*)$$

的整数. 而 $\mathbf{Z}$ 是交换环，

$$s6^2+p(6\cdot 9)+t9^2=(6s+9p)6+(9t)9$$

也具有(*)的形式. 同样

$$m6^3+n6^2\cdot 9+\cdots$$

也可以写成(*)的形式. 所以

$$\langle 6,\ 9\rangle=\{6k+9l \mid k,\ l\in \mathbf{Z}\}.$$

例题 2 在实数域 $\mathbf{R}$ 上 2 阶全阵环 $M_2(\mathbf{R})$ 中，求其子集

$$T=\left\{\begin{pmatrix}0 & m\\ n & 0\end{pmatrix}\,\middle|\, m,\ n\in \mathbf{Z}\right\}$$

生成的子环.

解 很明显，T 含于整数环 $\mathbf{Z}$ 上 2 阶全阵环 $M_2(\mathbf{Z})$. 任取

$$\begin{pmatrix}l & m\\ n & k\end{pmatrix}\in M_2(\mathbf{Z}),$$

由于

$$\begin{pmatrix}l & 0\\ 0 & k\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & k\\ l & 0\end{pmatrix}\in T,$$

知

$$\begin{pmatrix}l & m\\ n & k\end{pmatrix}=\begin{pmatrix}l & 0\\ 0 & k\end{pmatrix}+\begin{pmatrix}0 & m\\ n & 0\end{pmatrix}\in \langle T\rangle,$$

故有 $\langle T\rangle=M_2(\mathbf{Z})$.

设$(R, +, \cdot)$为一环，A为$(R, +)$的一个子群，则有商群

$$G/A = \{a + A, b + A, \cdots\}.$$

定义G/A的乘法，最自然的是令

$$(a + A)(b + A) = ab + A.$$

问题在于，A满足什么条件时，上述定义可与陪集的代表元选择无关呢？设

$$a + A = a_1 + A, \qquad b + A = b_1 + A,$$

则有$x, y \in A$使

$$a + x = a_1, \qquad b + y = b_1.$$

于是

$$a_1 b_1 = ab + ay + xb + xy.$$

欲使$a_1 b_1 + A = ab + A$，只要使

$$ay + xb + xy \in A$$

即可.

定义 3　设$(R, +, \cdot)$是个环，A是R的子集. 如果

1. $(A, +)$是$(R, +)$的子群；
2. 对任意$x, y \in A$和任意$a, b \in R$都有

$$ay, xb \in A,$$

则说A是R的**理想**.

我们用$A \leqslant R$表示A是R的子环，用$A \lhd R$表示A是R的理想. 从定义中可以看出，如果$A \lhd R$，则必有$A \leqslant R$. 因此，也有人称环的理想为环的理想子环.

条件 2 体现了对A的两侧要求，故有时称环的理想为其**双侧理想**或**两边理想**.

例 7　设I为环R的理想，则$M_n(I)$为$M_n(R)$的理想，$I[x]$为$R[x]$的理想.

设

$$A=\begin{pmatrix}a_{11} & \cdots & a_{1n}\\ \multicolumn{3}{c}{\cdots\cdots\cdots\cdots}\\ a_{n1} & \cdots & a_{nn}\end{pmatrix}\in M_n(I),$$

$$X=\begin{pmatrix}b_{11} & \cdots & b_{1n}\\ \multicolumn{3}{c}{\cdots\cdots\cdots\cdots}\\ b_{n1} & \cdots & b_{nn}\end{pmatrix}\in M_n(R),$$

因 $I\lhd R$ 知 $\sum a_{i\lambda}b_{\lambda j}$，$\sum b_{i\lambda}a_{\lambda j}\in I$，从而知 AX，$XA\in M_n(I)$. 此外，易知 $M_n(I)$ 为 $M_n(R)$ 的加法子群，故有 $M_n(I)\lhd M_n(R)$.

类似地，可得 $I[x]\lhd R[x]$.

例 8 在整数环 $\mathbf{Z}$ 中，偶数环是 $\mathbf{Z}$ 的理想.

例 9 在环 R 上多项式环 $R[x]$ 中，取定一个正整数 n，则集合

$$\left\{\sum_{i\geqslant n}a_ix^i\,\middle|\,a_i\in R\right\}$$

为 $R[x]$ 的理想.

例 10 集合

$$A=\left\{\begin{pmatrix}a & 0\\ b & 0\end{pmatrix}\,\middle|\,a,\ b\in\mathbf{Z}\right\}$$

是 $M_2(\mathbf{Z})$ 的子环，但不是其理想.

易验证 $A\leqslant M_2(\mathbf{Z})$. 注意

$$\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix}\in A,\quad \begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\in M_2(\mathbf{Z}),$$

但

$$\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}=\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\notin A,$$

即知 A 非 $M_2(\mathbf{Z})$ 的理想.

命题 7 设 R 是个环，A_α，$\alpha\in I$ 都是 R 的理想. 那么，它

们的交集$\bigcap_{\alpha\in I}A_\alpha$必然也是$R$的理想.

环R本身是R的理想. 因此, R的任一子集都包含在R的某些理想中. 此外, 设R的零元为0, 则$\{0\}$亦为R的理想. R与$\{0\}$都是R的平凡理想.

定义 4　设R是个环, $T\subseteq R$, T非空. 作R的理想族

$$B=\{I\lhd R,\ T\subseteq I\},$$

得到理想$\bigcap_{I\in B}I$称为R的由子集T**生成的理想**, 记为(T). 如果$T=\{a_1,\cdots,a_n\}$, 记$(T)=(a_1,\cdots,a_n)$, 称为由$a_1,\cdots,a_n$生成的理想. 称(a)为由a生成的**主理想**.

仿命题5, 可以证明

定理 1　设T是环R的非空子集. 那么, (T)中元恰由下述类型元组成:

$$n_1a_1+\cdots+n_ta_t+r_1b_1+\cdots+r_kb_k+c_1s_1+\cdots+c_ls_l+x_1d_1y_1+\cdots+x_id_iy_i,$$

其中$n_1,\cdots,n_t$是整数, $a_1,\cdots,a_t$, $b_1,\cdots,b_k$, $c_1,\cdots,c_l$, $d_1,\cdots,d_i\in T$, $r_1,\cdots,r_k$, $s_1,\cdots,s_t$, $x_1,\cdots,x_i$, $y_1,\cdots,y_i\in R$.

推论 1　设R是个环, $a\in R$. 则(a)恰由下列类型元组成

$$na+ra+as+x_1ay_1+\cdots+x_iay_i,$$

其中$n\in\mathbf{Z}$, r, s, $x_1,\cdots,x_i$, $y_1,\cdots,y_i\in R$.

特别, $(0)=\{0\}$. 常记$(0)=0$.

推论 2　设R是有1环, $a\in R$, 则

$$(a)=\left\{\sum x_iay_i\ \middle|\ x_i,\ y_i\in R\right\}.$$

注意, R无单位元时, 上式右端集合仍为R的理想, 记为RaR.

例题 3　整数环$\mathbf{Z}$中的每个子环S必定是由某个非负整数生成的主理想.

解　注意$(S,+)$为无限循环群$(\mathbf{Z},+)$的子群, 由第二章

§3 知有某非负整数 n 使

$$S = \{mn \mid m \in \mathbf{Z}\}.$$

而由定理 1 知上式右端恰为 (n).

设 A_i, $i \in I$ 都是环 R 的理想，$A = \bigcup_{i \in I} A_i$，称 (A) 为理想 A_i, $i \in I$ 的和，记为 $\sum_{i \in I} A_i$. 当 $I = \{\alpha, \beta, \cdots, \gamma\}$ 时，记 $\sum_{i \in I} A_i = A_\alpha + A_\beta + \cdots + A_\gamma$. 我们有

命题 8 设 A_i, $i \in I$ 都是环 R 的理想，则

$$\sum_{i \in I} A_i = \left\{ a \in R \,\middle|\, \text{有限集 } J \subseteq I \text{ 及 } a_i \in A_i, i \in J \text{ 使 } a = \sum_{i \in J} a_i \right\}.$$

证明 记上式右端集合为 S. 若 $a \in \sum A_i$，则有

$$T = \{a_1, \cdots, a_t, b_1, \cdots, b_k, c_1, \cdots, c_t, d_1, \cdots, d_i\} \subseteq A$$

及

$$n_1, \cdots, n_t \in \mathbf{Z}, r_1, \cdots, r_k, s_1, \cdots, s_t, x_1, \cdots, x_i, y_1, \cdots, y_i \in R$$

使

$$a = \sum n_\lambda a_\lambda + \sum r_\mu b_\mu + \sum c_\alpha s_\alpha + \sum x_\beta d_\beta y_\beta.$$

由 $A = \bigcup A_i$, $A_i \lhd R$，知上式右端多项式中每项均属于某个 A_i，故 $a \in S$. 反之，若 $a \in S$，则显然有 $a \in \sum A_i$. 总之有 $\sum A_i = S$.

例题 4 设 R 是有 1 交换环，给出 $a_1, \cdots, a_n \in R$ 生成的理想.

解 注意 R 有 1，又是交换环，用定理 1 有

$$(a_1, \cdots, a_n) = \{r_1 a_1 + \cdots + r_n a_n \mid r_1, \cdots, r_n \in R\},$$

$$(a_i) = \{r a_i \mid r \in R\}.$$

由命题 8，有

$$(a_1, \cdots, a_n) = (a_1) + \cdots + (a_n).$$

例题 5 设 R 为一环，则

$$A = \{x \in R \mid RxR = 0\}$$

为 R 的理想.

解 由于 $0 \in A$ 知 $A \neq \varnothing$. 设 $a, b \in A$, $r, s, t \in R$. 看

$$r(a-b)s = ras - rbs = 0 - 0 = 0,$$
$$s(ra)t = (sr)at = 0,$$
$$s(ar)t = sa(rt) = 0,$$

知 $A \lhd R$.

若 R 是有 1 环, 则 $A = \{0\}$. 若 R 是零乘环, 则 $A = R$. 若 R 是 §1 例 4 中的环, 则 $A = \{0, b\}$.

例题 6 设 A、B 为环 R 的非空子集. 通常用 AB 代表 R 中所有形如

$$a_1b_1 + \cdots + a_nb_n, \quad a_i \in , b_i \in B, n \in \mathbf{Z}, n \geqslant 1$$

元的集合. 证明, 如果 A, B 均为 R 的理想, 则 AB 也是 R 的理想.

解 由 A, B 非空, 知 $AB \neq \varnothing$. 设

$$a_1b_1 + \cdots + a_nb_n, \; c_1d_1 + \cdots + c_md_m \in AB, \quad u \in R,$$

其中 a_i, $c_i \in A$, b_i, $d_i \in B$, 那么

$$\begin{aligned}
&a_1b_1 + \cdots + a_nb_n - (c_1d_1 + \cdots + c_md_m) \\
&= a_1b_1 + \cdots + a_nb_n + (-c_1)d_1 + \cdots + (-c_m)d_m \in AB, \\
&u(a_1b_1 + \cdots + a_nb_n) \\
&= (ua_1)b_1 + \cdots + (ua_n)b_n \in AB, \\
&(a_1b_1 + \cdots + a_nb_n)u \\
&= a_1(b_1u) + \cdots + a_n(b_nu) \in AB,
\end{aligned}$$

故知 $AB \lhd R$.

例题 7 设

$$R = \left\{ A \in M_3(\mathbf{R}) \;\middle|\; A = \begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \right\},$$

$$S = \left\{ A \in R \,\middle|\, A = \begin{pmatrix} 0 & 0 & a \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix} \right\},$$

$$T = \left\{ A \in S \,\middle|\, A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & a \\ 0 & 0 & 0 \end{pmatrix} \right\}.$$

则 S 是环 R 的理想，T 是环 S 的理想，但 T 不是环 R 的理想.

解 显然，T 为 S 的子群，S 为 R 的子群，R 为一环. 记

$$A = \begin{pmatrix} 0 & a & b \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 0 & x \\ 0 & 0 & y \\ 0 & 0 & 0 \end{pmatrix},$$

$$C = \begin{pmatrix} 0 & 0 & ay \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad O = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & a \\ 0 & 0 & 0 \end{pmatrix}, \qquad E = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$F = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \qquad G = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

其中 $a, b, c, x, y \in R$. 由 $BD = DB = 0 \in T$, $D \in T$, $B \in S$ 可知 $T \lhd S$. 由 $AB = C \in S$, $BA = 0 \in S$, $A \in R$, $B \in S$，可知 $S \lhd R$. 但由 $EF = G \notin T$, $E \in R$, $F \in T$，知不是 R 的理想.

习　题

1. 设 p 是个素数. 证明，集合

$$H = \{ m/n \in \mathbf{Q} \mid (m, n) = 1 \text{ 且 } (n, p) = 1 \}$$

构成 $\mathbf{Q}$ 的一个子环，其中 (k, l) 表整数 k 与 l 的最高公因数.

2. 设 p 是个素数. 证明，集合

$$k = \{m/n \in \mathbf{Q} \mid (m, n) = 1 \text{ 且 } n = p^k, k \geqslant 0\}$$

构成 $\mathbf{Q}$ 的一个子环.

3. 给出 §1 例 4 中环 R 的所有子环.

4. 设 R 是个环. 那么

$$S = \{x \in R \mid \text{有 } n \in \mathbf{Z}, n \neq 0, \text{使 } nx = 0\}$$

构成 R 的一个理想.

5. 设 A 为 $R[x]$ 的一个非零理想，$f(x)$ 为 A 中次数最低者，则 $A = (f(x))$. 其中 $f(x)$ 次数的定义与数域上多项式次数的定义一致.

6. 设 I 为 $R[x]$ 的一个理想，n 为一自然数

$$I_n = \{a_n \mid \text{有 } a_0 + \cdots + a_n x^n \in I\},$$

证明：I_n 为 R 的理想.

7. 若 e_1、e_2 为交换环 R 的等方元，即

$$e_1^2 = e_1, \qquad e_2^2 = e_2,$$

证明，(e_1, e_2) 必为 R 的一个等方元生成的主理想.

§3 理想与商环(Ⅰ)

§2 引进理想的目有在于使商群为一环. 今证明之.

定理 1 设$(R, +, \cdot)$为一环，A 为 R 的一理想. 在商群 R/A 中定义乘法如下：对任意 $a+A$, $b+A \in R/A$，令

$$(a + A) \cdot (b + A) = ab + A,$$

则$(R/A, +, \cdot)$为一环.

证明 由理想定义前的说明知关于 R/A 的乘法的定义是合理的. 设 $a+A$, $b+A$, $c+A \in R/A$，则由

$$\begin{aligned}&[(a + A)(b + A)](c + A)\\ &= (ab + A)(c + A)\end{aligned}$$

$$=(ab)c+A$$
$$=a(bc)+A$$
$$=(a+A)(bc+A)$$
$$=(a+A)[(b+A)(c+A)],$$
$$(a+A)[(b+A)+(c+A)]$$
$$=(a+A)[(b+c)+A]$$
$$=a(b+c)+A$$
$$=(ab+ac)A$$
$$=(ab+A)+(ac+A)$$
$$=(a+A)(b+A)+(a+A)(c+A)$$

知 R/A 的乘法满足结合律，R/A 满足左分配律. 类似地还可证 R/A 满足右分配律，于是知 $(R/A,+,\cdot)$ 为一环.

定义 1 定理 1 中得到的 $(R/A,+,\cdot)$ 称为环 R 对理想 A 的**商环**，或称**剩余环**.

商环是环论的核心概念.

例 1 讨论整数环 $\mathbf{Z}$ 的所有商环.

任取 $A\lhd\mathbf{Z}$. 如果 $A=\mathbf{Z}$，则 $\mathbf{Z}/A$ 仅含一元是其零元. 如果 $A=0$，则 $\mathbf{Z}$ 中每一元 m 均对应商集 $\mathbf{Z}/A$ 中一个陪集 $\{m\}=m+\{0\}$，在商环中

$$(m+\{0\})+(n+\{0\})=(m+n)+\{0\}$$
$$(m+\{0\})(n+\{0\})=mn+\{0\}.$$

此环与 $\mathbf{Z}$ 无本质区别.

设 $A=(n)$. 上面讨论的是 $n=1$ 与 $n=0$ 的情形. 今设 $n>1$，则商集为

$$\mathbf{Z}/A=\{[0],[1],\cdots,[n-1]\},$$

其运算为

$$[a]+[b]=[a+b],\quad [a][b]=[ab].$$

特别地，取 $n=5$，则商环

$$\mathbf{Z}/(5) = \{[0],[1],[2],[3],[4]\}$$

的加法表与乘法表分别如下：

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

·	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

例 2 所有形如

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

的实 2 阶矩阵形成 $M_2(\mathbf{R})$ 的一个子环，记为 R. R 中所有形如

$$\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}$$

的矩阵集 A 是 R 的理想.

R 中任一元

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

恒可表为

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} + \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in A.$$

在 R/A 中，若

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + A = \begin{pmatrix} a_1 & 0 \\ 0 & b_1 \end{pmatrix} + A,$$

即

$$\begin{pmatrix} a - a_1 & 0 \\ 0 & b - b_1 \end{pmatrix} \in A,$$

则必有 $a=a_1$，$b=b_1$. 故知

$$R/A = \left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + A \,\middle|\, a, b \in \mathbf{R}\right\},$$

其运算为

$$\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + A\right) + \left(\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} + A\right) = \begin{pmatrix} a+c & 0 \\ 0 & b+a \end{pmatrix} + A,$$

$$\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + A\right)\left(\begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} + A\right) = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} + A.$$

例 3 设 $a \in \mathbf{R}$，

$$A = \{f(x) \mid f(x) \in \mathbf{R}[x], f(a) = 0\},$$

则 $A \lhd \mathbf{R}[x]$.

因 $f(a)=0$ 的充分必要条件是 $x-a \mid f(x)$，故

$$A = \{f(x) \mid f(x) \in \mathbf{R}[x], f(x) = (x-a)q(x), q(x) \in \mathbf{R}[x]\}.$$

任取 $h(x) \in \mathbf{R}[x]$，则有 $q(x) \in \mathbf{R}[x]$，$c \in \mathbf{R}$ 使

$$h(x) = q(x)(x-a) + c,$$

故有

$$h(x) + A = c + A.$$

若有 $d \in \mathbf{R}$ 使

$$c + A = d + A,$$

即 $c - d \in A$，则 $c = d$. 于是，商环

$$\mathbf{R}[x]/A = \{a + A \mid a \in \mathbf{R}\},$$

其运算为

$$(c+A) + (d+A) = (c+d)A,$$

$$(c+A)(d+A) = cd + A.$$

例题 1 设 R 是一环，子集

$$S = \{a \in R \mid a = xy - yx, x, y \in R\},$$

$C(R) = (S)$. 证明:$R/C(R)$是个交换环.

解 因为 $0 = 00 - 00 \in S$，故 $S \neq \varnothing$，(S)有意义. 任取 $u +$

$C(R)$, $v+C(R)\in R/C(R)$, 则有

$$(u+C(R))(v+C(R))-(v+C(R))(u+C(R))$$
$$=(uv-vu)+C(R)=C(R),$$

即

$$(u+C(R))(v+C(R))=(v+C(R))(u+C(R)),$$

知 $R/C(R)$ 为交换环.

如果环 R 不是零乘环, 又无非平凡理想, 则称 R 为**单纯环**或**单环**. 比如例 1 中的环

$$\{[0],[1],[2],[3],[4]\}$$

元数为 5, 其加法子群仅有其本身与 0, 从而其理想亦然, 故该环为单环.

例题 2　设 R 是个环, ~ 是 R 上一个等价关系, 而且 ~ 满足下列条件

1. 如果 $a\sim b$, 那么对任意 $c\in R$ 均有

$$a+c\sim b+c;$$

2. 如果 $a\sim b$, 那么对任意 $c\in R$ 均有

$$ac\sim bc,\qquad ca\sim cb.$$

证明, 零元所在的等价类

$$K=\{x\in R\mid x\sim 0\}$$

是 R 的一个理想.

证明　对任意 a, $b\in K$ 及 $r\in R$, 由

$$a-b=a+(-b),\quad b\sim 0$$

知 $a-b\sim a$, $a-b\sim 0$. 同时, 由 $a\sim 0$ 知

$$ra\sim r0,\quad r0=0,\quad ra\sim 0$$
$$ar\sim 0r,\quad 0r=0,\quad ar\sim 0$$

这说明 K 是 R 的一个理想.

例题 3　记偶数环为 E, 则 $M_2(E)\lhd M_2(\mathbf{Z})$. 给出商环 $M_2(\mathbf{Z})/M_2(E)$ 的结构.

解 由 §2 例 8 知 $E \lhd \mathbf{Z}$，由 §2 例 7 知 $M_2(E) \lhd M_2(\mathbf{Z})$. 令

$$D_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

$$D_2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad D_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

$$D_4 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad D_5 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},$$

$$D_6 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad D_7 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$D_8 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad D_9 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix},$$

$$D_{10} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad D_{11} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

$$D_{12} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad D_{13} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

$$D_{14} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad D_{15} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},$$

并用 $\overline{D}_i$ 代表商环 $M_2(\mathbf{Z})/M_2(E)$ 中元 $D_i + M_2(E)$. 因为每个整数都可写成 $2n+0$ 或 $2n+1$ 的形式，知 $A \in M_2(\mathbf{Z})$ 总可写成

$$D_i + B, \quad B \in M_2(E)$$

的形式，于是有 $A + M_2(E) = D_i + M_2(E)$. 易验证 $i \neq j$ 时

$$D_i + M_2(E) \neq D_j + M_2(E).$$

故

$$M_2(\mathbf{Z})/M_2(E) = \{\overline{D}_0, \overline{D}_1, \overline{D}_2, \overline{D}_3, \overline{D}_4, \overline{D}_5, \overline{D}_6, \overline{D}_7, \overline{D}_8, \overline{D}_9, \overline{D}_{10}, \overline{D}_{11}, \overline{D}_{12}, \overline{D}_{13}, \overline{D}_{14}, \overline{D}_{15}\},$$

其加法与乘法举例如下

$$\overline{D}_1 + \overline{D}_2 = \overline{D}_3, \qquad \overline{D}_1\overline{D}_2 = \overline{D}_2,$$

其要点是，按一般矩阵的加法与乘法运算，得到的矩阵的元为 0，1 时照写，得到的是 2 时改为 0.

习　　题

1. $\mathbf{Z}/(9)$ 中哪些元是单位？哪些是零因子？哪些元(加法)周期是 3？哪些元的(加法)周期是 9？

2. 证明，$\mathbf{Z}/(6)$ 中含有单位的子环只有 $\mathbf{Z}/(6)$.

3. 设 e 是环 R 的单位元，$I \triangleleft R$. 证明 $e+I$ 是商环 R/I 的单位元. 进一步问，若 $I \triangleleft R$，R/I 有单位元，则 R 一定有单位元吗？

4. 设 I 为环 R 的理想，$I \neq R$. 如 R 无零因子，则 R/I 一定无零因子吗？如 R/I 无零因子，R 一定无零因子吗？

5. 设 I 为环 R 的理想. 若 I 的每个元的加法周期都有限，且 R/I 的每个元的加法周期有限，则 R 的每个元的加法周期都有限.

6. 设 R 为一环，R 不是零乘环，R 的元数是一素数. 求证 R 为单环.

7*. 设 R 为有 1 环，$K \triangleleft M_n(R)$. 证明，必有 $N \triangleleft R$ 使 $K = M_n(N)$.

§4　环的同态映射

群的同态映射反映了两个群结构的相似性. 对于环，则有

定义 1　设 R 和 S 都是环. R 到 S 的映射 φ 称为 R 到 S 的(环)**同态映射**，如果对任意 $a, b \in R$ 恒有

$$\varphi(a+b) = \varphi(a) + \varphi(b),$$
$$\varphi(ab) = \varphi(a)\varphi(b),$$

此时，称 R 在 φ 下同态于 S. 如果 φ 还是满射，则称 S 是 R 的

同态象. 如果 φ 还是双射, 则称 φ 是 R 到 S 的**同构映射**, 此时称 R 和 S 是同构的, 记为 $R\cong S$.

与群的情形类似, 可以证明, 如果 φ 是 R 到 S 的同构映射, 则 φ 的逆映射 φ^{-1} 是 S 到 R 的同构映射.

例 1 设 $a\in\mathbf{R}$, 令

$$\varphi: f(x)\rightarrow f(a),$$

则 φ 是 $\mathbf{R}[x]$ 到 $\mathbf{R}$ 的一个环同态.

若 $b\in\mathbf{R}$, 则取

$$f(x)=x+(b-a),$$

于是有 $\varphi(f(x))=b$, 知 φ 是满的.

例 2 在 §3 例 2 的环 R 中, 令

$$\varphi:\begin{pmatrix}a & c\\ 0 & b\end{pmatrix}\rightarrow\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix},$$

则 φ 是 R 到自身的同态, 称为自同态. 它不是满射, 因为 R 中任意矩阵在 φ 之下均不对应矩阵

$$\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}.$$

而且, φ 也不是单射, 因为

$$\varphi\left(\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\right)=\varphi\left(\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}\right)=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}.$$

设 φ 是环 $(R,+,\cdot)$ 到环 $(S,+,\cdot)$ 的环同态映射, 那么, φ 当然是群 $(R,+)$ 到群 $(S,+)$ 的群同态映射. 于是有

1. $\varphi(0)=0$,
2. $\varphi(a-b)=\varphi(a)-\varphi(b)$, $a,b\in R$,
3. $\varphi(ma)=m\varphi(a)$, $m\in I$, $a\in R$,
4. φ 是单射的充分必要条件是 $\mathrm{Ker}(\varphi)=\{0\}$.

对于环同态映射的象与核, 我们有

命题 1 设 φ 是环 R 到环 S 的同态. 如果 A 是 R 的子环,

则 $\varphi(A)$ 是 S 的子环. 特别, $\mathrm{Img}(\varphi)$ 是 S 的子环. 如果 A 是 R 的理想而 φ 是满射, 则 $\varphi(A)$ 是 S 的理想.

证明　由第三章 §2 命题6 知 $\varphi(A)$ 为 S 的子群. 设 $x, y \in \varphi(A)$, 则有 $a, b \in A$ 使 $x = \varphi(a)$, $y = \varphi(b)$, 从而有

$$xy = \varphi(a)\varphi(b) = \varphi(ab) \in \varphi(A),$$

故 $\varphi(A) \leqslant S$. 若 φ 是满的而 $A \lhd R$, 可设上式中的 $x \in S$, $a \in R$, 可知 $\varphi(A) \lhd S$.

一般地, $\mathrm{Img}(\varphi)$ 未必是 S 的理想. 看例3,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \in \mathrm{Img}(\varphi),$$

但

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \notin \mathrm{Img}(\varphi).$$

命题2　设 φ 是环 R 到 S 的同态. 如果 R 有单位元 e, 则环 $\mathrm{Img}(\varphi)$ 必有单位元, 而且恰为 $\varphi(e)$. 特别, 如果 φ 是满射, 则 $\varphi(e)$ 是 S 的单位元.

证明　设 $\varphi(a) \in \mathrm{Img}(\varphi)$, 其中 $a \in R$. 由于

$$\varphi(e)\varphi(a) = \varphi(ea) = \varphi(a),$$
$$\varphi(a)\varphi(e) = \varphi(ae) = \varphi(a),$$

知 $\varphi(e)$ 为 $\mathrm{Img}(\varphi)$ 的单位元. 而在第一章中已证明过, 对于集合上满足结合律的二元运算, 如果有恒等元, 则必唯一. 故 $\varphi(e)$ 恰为 $\mathrm{Img}(\varphi)$ 的单位元.

如果 φ 不是满射, 则 $\varphi(e)$ 未必是 S 的恒等元. 例如, 取 R 为 $M_2(\mathbf{R})$ 中全部对角矩阵形成的子环, 而 S 为 $M_2(\mathbf{R})$ 中所有形如

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \quad a \in \mathbf{R}$$

的矩阵形成的子环, 映射

$$\varphi:\begin{pmatrix}a & c\\0 & b\end{pmatrix}\to\begin{pmatrix}a & 0\\0 & 0\end{pmatrix}$$

显然是 R 到 S 的环同态. 元

$$\varphi(e)=\varphi\left(\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$$

恰为 S 的单位元. 但是, φ 也定义了 R 到 R 的环同态, 而 $\varphi(e)$ 却不是 R 的单位元.

可以仿照群中的证法证明

命题 3 设 φ 是环 R 到环 S 的同态, ψ 是环 S 到环 K 的同态. 那么, 复合映射 $\psi\circ\varphi$ 是环 R 到环 K 的同态.

命题 4 设 φ 是环 R 到环 S 的同态. 那么 φ 的核 $\mathrm{Ker}(\varphi)$ 是环 R 的理想.

证明 $\mathrm{Ker}(\varphi)$ 也是 $(R,+)$ 到 $(S,+)$ 的群同态 φ 的核, 故为 $(R,+)$ 的子群. 若 $a\in\mathrm{Ker}(\varphi)$, $r\in R$, 则

$$\varphi(ar)=\varphi(a)\varphi(r)=0\varphi(r)=0,$$

同理有 $\varphi(ra)=0$, 即 ar, $ra\in\mathrm{Ker}(\varphi)$, 知 $\mathrm{Ker}(\varphi)\lhd R$.

仿群论的证明还可得到

定理 1 如果 A 是环 R 的理想, 则

$$\varphi: r\to r+A$$

是环 R 到环 R/A 的满的同态(称为 R 到 R/A 的自然映射). 反之, 如果 φ 是环 R 到 S 的满同态, $\mathrm{Ker}(\varphi)=A$, 那么

$$r+A\to\varphi(r)$$

是环 R/A 到环 S 的同构映射.

例题 1 设 φ 是环 R 到环 S 的同态映射. 若 A 是 S 的子环, 则 $\varphi^{-1}(S)$ 是 R 的子环; 若 A 是 S 的理想, 则 $\varphi^{-1}(A)$ 是 R 的理想.

解 由第三章 §2 命题6 知 $\varphi^{-1}(A)$ 为 R 的子群. 设 x, $y\in\varphi^{-1}(A)$, 则 $\varphi(x)$, $\varphi(y)\in A$, 从而有

$$\varphi(xy)=\varphi(x)\varphi(y)\in A,\quad x,y\in\varphi^{-1}(A),$$

故 $\varphi^{-1}(A)\leqslant R$. 当 $A\lhd S$ 时，对上式中 x, y 中的一个使之为 R 中元，则仍有 $xy\in\varphi^{-1}(A)$，故

$$\varphi^{-1}(A)\lhd R.$$

定理 2　设 φ 是环 R 到环 R'的满同态，那么，在$(R,+)$的包含 $\mathrm{Ker}(\varphi)$ 的子群集与 R' 的子群集间的一一对应 $H\to\varphi(H)$，H 是 R 的子环的充分必要条件是 $\varphi(H)$ 是 R'的子环，H 是 R 的理想的充分必要条件是 $\varphi(H)$ 是 R'的理想. 此外，如果 I 是 R 的包含 $\mathrm{Ker}(\varphi)$ 的理想，则

$$a+I\to\varphi(a)+I',\quad I'=\varphi(I)$$

是环 R/I 与环 R'/I'的同构映射.

证明　设 H'为加群 R'的子群，用第三章 §2 命题 8，知

$$\varphi^{-1}(H')\to\varphi(\varphi^{-1}(H'))=H'\cap\mathrm{Img}(\varphi)=H'\cap R'=H'.$$

若 H_1, H_2 均为 R 的含 $\mathrm{Ker}(\varphi)$ 的子群且 $\varphi(H_1)=\varphi(H_2)$，还用刚提到的命题 8，有

$$\begin{aligned}H_1&=H_1+\mathrm{Ker}(\varphi)\\&=\varphi^{-1}(\varphi(H_1))=\varphi^{-1}(\varphi(H_2))\\&=H_2+\mathrm{Ker}(\varphi)=H_2.\end{aligned}$$

所以，$H\to\varphi(H)$ 是一一对应. 再由本节命题 1，例题 1 知，只需证定理的最后一个断言. 我们还知道，$a+I\to\varphi(a)+I'$为加群 R/I 与 R'/I'的同构. 注意

$$\begin{aligned}(a+I)(b+I)&=ab+I=\varphi(ab)+I'\\&=\varphi(a)\varphi(b)+I'\\&=(\varphi(a)+I')(\varphi(b)+I'),\end{aligned}$$

知 $a+I\to\varphi(a)+I'$还是环的同构.

此定理通常称为环的第二同构定理. 下边的定理是环的第一同构定理.

定理 3　设 R 是个环，S 是 R 的一个子环，I 是 R 的一个理

想. 那么, $S+I=\{s+i \mid s\in S,\ i\in I\}$为$R$的子环, 它含$I$作为理想, $S\cap I$是S的一个理想, 而映射

$$s+I\to s+(S\cap I),\quad s\in S$$

是环$(S+I)/I$到环$S/(S\cap I)$的同构.

证明 由于$I\lhd R$, 易知$S+I\leqslant R$, $I\lhd S+I$, 从而$(S+I)/I$为一环. 从R到R/I的自然映射可导出S到R/I的同态$s\to s+I$, 其象为$S+I$, 而核为$S\cap I$. 由定理1知$s+(S\cap I)\to s+I$为环$S/(S\cap I)$与环$(S+I)/I$的同构. 故其逆映射为$(S+I)/I$与$S/(S\cap I)$的同构.

例3 例1中的

$$\varphi: f(x)\to f(a)$$

是$\mathbf{R}[x]$到$\mathbf{R}$的满同态, 核

$$\mathrm{Ker}(\varphi)=\{f(x)\in\mathbf{R}[x]\mid f(a)=0\}.$$

由§3例3知

$$\mathrm{Ker}(\varphi)=\{f(x)\in\mathbf{R}[x]\mid x-a\mid f(x)\},$$

利用§2定理1推论2, 注意$\mathbf{R}[x]$的交换性, 知

$$\mathrm{Ker}(\varphi)=(x-a).$$

由定理1知

$$\mathbf{R}[x]/(x-a)\cong\mathbf{R}.$$

例4 记

$$R=\left\{K\in M_2(\mathbf{R})\,\middle|\,K=\begin{pmatrix}a & c\\ 0 & b\end{pmatrix}\right\},$$

$$S=\left\{K\in M_2(\mathbf{R})\,\middle|\,K=\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}\right\},$$

则

$$\varphi:\begin{pmatrix}a & c\\ 0 & b\end{pmatrix}\to\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}$$

为R到S的满同态, 而

$$\mathrm{Ker}(\varphi) = \left\{K \in M_2(\mathbf{R}) \,\middle|\, K = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}\right\},$$

$$R/\mathrm{Ker}(\varphi) \cong S.$$

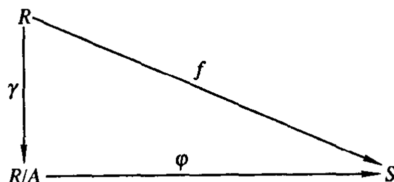
例 5　设 f 是环 R 到环 S 的满同态，$\mathrm{Ker}(f) = A$，再设

$$\theta: r \to r + A$$

为 R 到 R/A 的自然映射，则

$$\varphi: r + A \to f(r)$$

为 R/A 到 S 的同构. 与群的情形类似，有环同态的等式 $f = \varphi \circ r$，也就是下面的图形可换.



例题 2　设 R 是个环，S 是个集合，φ 是 R 到 S 的一个双射，φ^{-1} 是 φ 的逆映射. 对任意 $a, b \in S$，令

$$a + b = \varphi[\varphi^{-1}(a) + \varphi^{-1}(b)],$$

$$ab = \varphi[\varphi^{-1}(a)\varphi^{-1}(b)],$$

则 $(S, +, \cdot)$ 是个环，φ 是环 R 到环 S 的同构.

解　首先注意到，任取 $a, b \in S$，因 φ^{-1} 是映射，有确定的

$$\varphi^{-1}(a), \varphi^{-1}(b) \in R.$$

而 R 是环，又有确定的

$$\varphi^{-1}(a) + \varphi^{-1}(b), \varphi^{-1}(a)\varphi^{-1}(b).$$

再由 φ 为映射知

$$\varphi[\varphi^{-1}(a) + \varphi^{-1}(b)], \quad \varphi[\varphi^{-1}(a)\varphi^{-1}(b)]$$

为 S 中确定的元素，从而 $+$，$\cdot$ 为 S 上两个二元运算.

要验证各种算律都极容易，仅以右分配律为例说明之. 任

取 $a, b, c \in S$，必有

$$
\begin{aligned}
&(a+b)c \\
&= \varphi[\varphi^{-1}(a+b)\varphi^{-1}(c)] \\
&= \varphi[\varphi^{-1}(\varphi[\varphi^{-1}(a)+\varphi^{-1}(b)])\varphi^{-1}(c)] \\
&= \varphi[\varphi^{-1}(a)+\varphi^{-1}(b)\varphi^{-1}(c)] \\
&= \varphi[\varphi^{-1}(a)\varphi^{-1}(c)+\varphi^{-1}(b)\varphi^{-1}(c)] \\
&= \varphi[\varphi^{-1}\varphi(\varphi^{-1}(a)\varphi^{-1}(c))+\varphi^{-1}\varphi(\varphi^{-1}(b)\varphi^{-1}(c))] \\
&= \varphi[\varphi^{-1}(a)\varphi^{-1}(c)]+\varphi[\varphi^{-1}(b)\varphi^{-1}(c)] \\
&= ac+bc.
\end{aligned}
$$

类似地可验证，若 0 是 R 的零元，则 $\varphi(0)$ 为 S 的零元，而对 $a \in S$，$\varphi[-\varphi^{-1}(a)]$ 为 a 的负元. 故 $(S, +, \cdot)$ 为一环.

对任意 $a', b' \in R$，设 $\varphi(a')=a$，$\varphi(b')=b$，则

$$
\begin{aligned}
\varphi(a'+b') &= \varphi[\varphi^{-1}\varphi(a')+\varphi^{-1}\varphi(b')] \\
&= \varphi(a')+\varphi(b'), \\
\varphi(a'b') &= \varphi[\varphi^{-1}(a')\varphi^{-1}\varphi(b')] \\
&= \varphi(a')\varphi(b'),
\end{aligned}
$$

知双射 φ 为环 R 到环 S 的同构.

例题 3 设

$$
S' = \left\{ A \in M_4(\mathbf{R}) \,\middle|\, A = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \right\},
$$

$$
I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad I = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix},
$$

$$J=\begin{pmatrix}0&0&-1&0\\0&0&0&1\\1&0&0&0\\0&-1&0&0\end{pmatrix},\quad K=\begin{pmatrix}0&0&0&-1\\0&0&-1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}.$$

对任意 $A\in S'$，有 $a, b, c, d\in \mathbf{R}$ 使

$$A=aI_4+bI+cJ+dK,$$

故 S'对矩阵减法是封闭的.

看 I_4, I, J, K 的乘法表

	I_4	I	J	K
I_4	I_4	I	J	K
I	I	$-I_4$	K	$-J$
J	J	$-K$	$-I_4$	I
K	K	J	$-I$	$-I_4$

易知 S'对矩阵乘法也是封闭的，这说明 S'是个以 I_4 为单位元的环.

再看

$$S=\left\{x\in M_2(\mathbf{C})\,\middle|\,x=\begin{pmatrix}a+b\sqrt{-1}&c+d\sqrt{-1}\\-c+d\sqrt{-1}&a-b\sqrt{-1}\end{pmatrix},\ a, b, c, d\in\mathbf{R}\right\},$$

$$e=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad i=\begin{pmatrix}\sqrt{-1}&0\\0&-\sqrt{-1}\end{pmatrix},$$

$$j=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad k=\begin{pmatrix}0&\sqrt{-1}\\\sqrt{-1}&0\end{pmatrix},$$

则 S 也是个环. 证明 S'环同构于环 S.

证明 令

$$\varphi: S' \to S$$

$$\varphi: aI_4 + bI + cJ + dK \to ae + bi + cj + dk$$

可以证明这是个双射. 再由 I_4, I, J, K 的乘法表与 e, i, j, k 乘法表间的对应，即可看出 φ 是保乘映射，从而知 φ 是同构映射.

习 题

1. 求本节例 2 中环 R 的自同态

$$\sigma: \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \to \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

的核. 令

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix},$$

求原象 $\varphi^{-1}(\{A\})$, $\varphi^{-1}(\{B\})$.

2. 设 f, g 都是从 $\mathbf{Q}$ 和 $\mathbf{R}$ 的同态，且对每个 $i \in \mathbf{Z}$，恒有 $f(i) = g(i)$. 证明，f 和 g 是 $\mathbf{Q}$ 上相同的映射，即对每个 $x \in \mathbf{Q}$ 有 $f(x) = g(x)$.

3. 设 T 是所有形如

$$a + b\sqrt{3}, \quad a, b \in \mathbf{Z}$$

的实数做成的 $\mathbf{R}$ 的子环，令

$$f: a + b\sqrt{3} \to a - b\sqrt{3},$$

说明 f 是 T 的自同态. 求出 $\mathrm{Ker}(f)$, $\mathrm{Img}(f)$.

4. 设 φ 是环 R 到环 S 的同态. 证明：R 为交换环时 $\mathrm{Img}(\varphi)$ 亦为交换环.

5. 设 R 为一环，S 是带 +，· 两种运算的集合，φ 是 R 到 S 的映射. 若对任意 a, $b \in R$，恒有

$$\varphi(a + b) = \varphi(a) + \varphi(b), \qquad \varphi(ab) = \varphi(a) \cdot \varphi(b),$$

则 $\mathrm{Img}(\varphi)$ 为一环，φ 是环 R 到 $\mathrm{Img}(\varphi)$ 的同态.

§5 理想与商环(Ⅱ)

定义 1 设 $(R, +, \cdot)$ 是个至少含两个元素的环，用 R_0 代表 R 中所有非零元的集合. 如果 $(R_0, \cdot)$ 为一群，则说 $(R, +, \cdot)$ 是个除环，简单地说 R 是个**除环**. 如除环 R 又是交换环时，说 R 是个**域**.

有人称除环为体、除体、斜域，称域为交换除环域交换体.

例 1 对任意 $f(x) \in \mathbf{R}[x]$，用 x^2+1 去除，有 $g(x) \in \mathbf{R}[x]$，$\alpha, \beta \in \mathbf{R}$ 使

$$f(x) = g(x)(x^2+1) + \alpha x + \beta,$$

令

$$\varphi: f(x) \to \alpha \mathrm{i} + \beta, \quad \mathrm{i} = \sqrt{-1},$$

易验证 φ 是 $\mathbf{R}[x]$ 的 $\mathbf{C}$ 的满同态. 注意 $\varphi(f(x)) = 0$ 的充分必要条件是 $\alpha i + \beta = 0$，等价于 $\alpha x + \beta = 0$，等价于 $(x^2+1) \mid f(x)$，等价于 $f(x) \in (x^2+1)$. 故知 $\mathrm{Ker}(\varphi) = (x^2+1)$，由同态基本定理知

$$\mathbf{R}[x]/(x^2+1) \cong \mathbf{C}.$$

上例 说明，$\mathbf{R}[x]$ 对理想 (x^2+1) 的剩余环为域. 那么，$\mathbf{R}[x]$ 有无真理想(即非平凡理想) A 使 $\mathbf{R}[x]/A$ 不是域呢？

例 2 设 $f(x) \in \mathbf{R}[x]$，$A = (x^2-1)$，用 $\overline{f(x)}$ 代表 $\mathbf{R}[x]/A$ 中 $f(x)$ 所在的陪集 $f(x) + A$. 由 $x-1 \notin A$ 知 $\overline{x-1} \neq 0 = A$. 同样有 $\overline{x+1} \neq 0$，但 $(x+1)(x-1) = x^2-1 \in A$，即

$$\overline{x-1} \cdot \overline{x+1} = 0.$$

记 $R = \mathbf{R}[x]/A$，则 R_0 关于乘法不封闭，R_0 非群，R 不是除环.

例 3 在 $\mathbf{R}[x]$ 中无真含 (x^2+1) 的真理想，而 $\mathbf{R}[x]$ 的真

理想$(x-1)$真包含(x^2-1).

由§4定理2及

$$\mathbf{R}[x]/(x^2+1)\cong\mathbf{C}$$

知$\mathbf{R}[x]$无真包(x^2+1)的真理想. 而且$(x-1)$其包含(x^2-1).

若I是环$\mathbf{R}$的一个理想，且对$\mathbf{R}$的任意理想J，只要$I\leqslant J$，$I\neq J$，则必有$J=\mathbf{R}$，称I为$\mathbf{R}$的一个**极大理想**.

例4 单环R中$\{0\}$为其极大理想.

例题1* R代表有理数加群$\mathbf{Q}$上的零乘环·那么，R无极大理想.

解 $\mathbf{Q}$的每一个加法子群恰为R的一个理想. 设A是R的一个极大理想，有$q\in R$，$q\notin A$. 于是$(q)+A$真包含A，由A的极大性，有

$$(q)+A=R. \tag{1}$$

由于q是个有理数，$\frac{1}{2}q\in R$(也就是$\mathbf{Q}$). 于是，由(1)必有$z\in\mathbf{Z}$，$a\in A$使

$$\frac{q}{2}=zq+a,$$

进而有

$$(1-2z)q=2a.$$

但是，$1-2z\in\mathbf{Z}$，$\frac{1}{1-2z}\in\mathbf{R}$. 再利用(1)又应有$z_1\in\mathbf{Z}$，$a_1\in A$使

$$\frac{q}{1-2z}=z_1q+a_1.$$

导致

$$q=(1-2z)qz_1+(1-2z)a_1=2z_1a+(1-2z)a_1\in A,$$

矛盾.

设 A 为环 R 的理想. 由上节定理 2 知, R/A 为单环当而且仅当 A 为 R 的极大理想且 R/A 不是零乘环.

命题 1　交换的单环 R 为域.

证明　记 R 的非零元集为 R_0, 由 $R^2 \neq 0$ 知 R_0 非空, R 含两元以上. 设 $a \in R_0$, 易验证 $aR \lhd R$, $A = \{r \in R \mid rR = 0\} \lhd R$. 若 $aR = 0$, 则 $A \neq 0$, 从而 $A = R$, 导致 $R^2 = AR = 0$, 矛盾. 故 $aR \neq 0$, 从而有 $aR = R$. 即对任意 a, $b \notin R_0$ 恒有 $c \in R$ 使 $ac = b$. 若 $c = 0$, 则 $b = 0$, 与 $b \in R_0$ 矛盾. 故 $c \in R_0$. 由第二章 §1 知 R_0 为一群, 从而 R 为域.

定理 1　设 A 为 1 交换环 R 的理想, 则 R/A 为域的充分必要条件是 A 为 R 的极大理想.

证明　由 R 有单位元知 $A \neq R$ 时 R/A 亦有单位元, 从而知它不是零乘环. 再用命题 1 即可.

例 5　若

$$f(x) = q(x)(x+1) + r, \quad f(x), q(x) \in \mathbf{R}[x], r \in \mathbf{R},$$

令

$$\varphi: f(x) = r.$$

易验证 φ 是 $\mathbf{R}[x]$ 到 $\mathbf{R}$ 的满同态, 核为 $(x+1)$, 从而

$$\mathbf{R}[x]/(x+1) \cong \mathbf{R},$$

由定理 1 知 $(x+1)$ 为 $\mathbf{R}[x]$ 的一个极大理想.

同理, 由例 1 可直接知道 (x^2+1) 为 $\mathbf{R}[x]$ 的一个极大理想. 此证明比例 2 的证明简单.

我们知道, A 为环 R 的极大理想时, R/A 可能是单环. 以下讨论, 当 $A \lhd R$ 时, R/A 在什么条件下是无零因子环、有 1 环、交换环, 等等.

定义 2　设 R 是个交换环, P 是 R 的一个理想. 如果 $P \neq R$ 且对任意 a, $b \in R$, $ab \in P$ 蕴涵 $a \in P$ 或 $b \in P$, 则说 P 是 R 的一个**素理想**.

如果 0 是 R 的素理想，则说 R 是个**素环**.

例如，环 R 是交换的无零因子环时，0 是 R 的一个素理想，R 是素环.

又如，p 为素数时，(p)是 $\mathbf{Z}$ 的素理想. 因为，当 $m, n \in \mathbf{Z}$ 且 $mn \in (p)$时，mn 为 p 的整数倍，$p \mid mn$，从而有 $p \mid m$ 或 $p \mid n$，即 $m \in (p)$或 $n \in (p)$.

命题 2 设 P 为交换环 R 的理想且 $P \neq R$. 那么，P 为 R 的素理想的充分必要条件是 R/P 不含零因子.

证明 设有 $a, b \in R$ 使 $ab \in P$，则

$$(a+P)(b+P) = ab+P = P.$$

若 R/P 不含零因子，则有 $a+P=P$ 或 $b+P=P$，从而有 $a \in P$ 或 $b \in P$，P 为 R 的素理想.

反之，设 P 为 R 的素理想，若有 $a, b \in R$ 使

$$(a+P)(b+P) = P,$$

即

$$ab+P = P,$$

则 $ab \in P$，从而有 $a \in P$ 或 $b \in P$，即 $a+P=P$ 或 $b+P=P$，R/P 中无零因子.

例 6 设 A 为有 1 交换环 R 的极大理想，则 A 为 R 的素理想.

由定理知 R/A 为域，从而无零因子，再用命题 2 即可.

命题 3 设 A 为环 R 的理想. 那么，R/A 为交换环的充分必要条件是对任意 $x, y \in R$，均有 $xy-yx \in A$.

证明 R/A 为交换环的充分必要条件是对任意 $x, y \in R$ 均有

$$xy+A = (x+A)(y+A) = (y+A)(x+A) = yx+A,$$

这等价于：对任意 $x, y \in R$ 恒有

$$xy-yx \in A.$$

例题 2　设 R 是个交换环. 对任意 $a\in R$, 易验证

$$N_a=\{x\in R\mid x=ar-r,\ r\in R\}$$

是 R 的理想. 证明, R 的理想 $A\neq R$ 使 R/A 有单位元的充分必要条件是有 $e\in R$ 使 $N_e\subseteq A$.

解　R/A 有单位元等价于有 $e\in R$ 对任意 $r\in R$ 均有

$$er+A=(e+A)(r+A)=r+A,$$

等价于有 $e\in R$ 对任意 $r\in R$ 均有 $er-r\in A$, 等价于 $e\in R$ 使 $N_e\subseteq A$.

当环 R 有单位元 1 时, $N_1=0$, 它含在每个理想里, 故 R 的每个商环都是有单位元的. 这一点, 在讨论环的同态象时, 已经说过了.

例题 3*　设 R 为一环. $a\in R$ 被称为幂零的, 如有正整数 n 使 $a^n=0$. 证明, 交换环 R 的所有幂零元集 N 是 R 的一个理想, 而 R/N 无非零幂零元.

解　因为 $0\in N$ 知 $N\neq\varnothing$. 设 $a,b\in N$, 则有 $m,n\in\mathbf{Z}$ 使 $a^m=b^n=0$, 从而有

$$\begin{aligned}&(a-b)^{m+n}\\&=a^{m+n}+(m+n)a^{m+n-1}b+\cdots+(m+n)ab^{m+n-1}+b^{m+n}\\&=0,\end{aligned}$$

(等式中 a^ib^j 中或者 $i\geqslant m$, 或者 $j\geqslant n$) 故 $a-b\in N$. 再设 $r\in R$, 则

$$(ar)^m=a^mr^m=0,$$

故 $ar\in N$, $N\lhd R$.

设 $a+N$ 为 R/N 的一个幂零元, 即有 $m\in\mathbf{Z}$ 使

$$(a+N)^m=N.$$

于是有 $a^m+N=N$, 即 $a^m\in N$. 故有 $n\in\mathbf{Z}$ 使 $(a^m)^n=0$, 知 $a\in N$, 从而 $a+N=N$, R/N 无非零幂零元.

欲得到环的具有某种性质的同态象, 往往考虑环中那些破

坏此性质的元生成的理想，再将环对此理想作商环. 这种方法在抽象代数学中很有用.

在第三章我们学习了群的直积，今看环的直和.

设 R_1, R_2, …, R_n 均为环. 按第三章§5，它们作为交换群（仅论其加法运算）可得一外直积 $\prod_{i=1}^{n} R_i$，具体运算是

$$(a_1,\cdots,a_n)+(b_1,\cdots,b_n)=(a_1+b_1,\cdots,a_n+b_n)$$

其中 a_i, $b_i \in R_i$. 现在，我们把这个积称为和，把 $\prod_{i=1}^{n} R_i$ 记为 $R_1 \oplus \cdots \oplus R_n = R$，或 $\bigoplus_{i=1}^{n} R_i = R$.

再利用诸 R_i 的乘法，规定

$$(a_1,\cdots,a_n)(b_1,\cdots,b_n)=(a_1b_1,\cdots,a_nb_n),$$

很容易验证 $R_1 \oplus \cdots \oplus R_n$ 在这样的加和乘之下是个环. 我们称为环 R_1, …, R_n 的外直和. 对于无穷多个，以 I 为指标集的环族

$$\{R_i \mid i \in I\}$$

可仿群论中的思路，定义 $\prod_{i \in I} R_i$ 为结合环.

同样，如同在群论中的内直积，有

定义 3 设 $R_i(i=1,2,\cdots,n)$ 是环 R 的理想. 如果

1. $R=\sum_{i=1}^{n} R_i = R_1+R_2+\cdots+R_n$,

2. 对任意 $r \in R$，表成

$$r = r_1+\cdots+r_n, \quad r_i \in R_i$$

时，表法唯一.

则说 R 是 R_1, …, R_n 的（内）直和，也记成 $R=\bigoplus_{i=1}^{n} R_i$（容易证明，此时同构于诸 R_i 的外直和）.

命题 5 设 $R_i(i=1,\cdots,n)$ 都是环 R 的理想，且 $R=R_1+\cdots$

$+R_n$，那么 $R=\bigoplus_{i=1}^{n} R_i$ 的充分必要条件是

$$0=r_1+\cdots+r_n,\quad r_i\in R_i$$

时表法唯一，即 $r_i=0$，$i=1,2,\cdots,n$.

证明　必要性显然. 如果 $R=R_1+\cdots+R_n$，且 0 的表法唯一，那么，对任意 $r\in R$，设有

$$r=r_1+r_2+\cdots+r_n,\quad r_i\in R_i$$

$$r=s_1+s_2+\cdots+s_n,\quad s_i\in R_i$$

两式相减得

$$0=(r_1-s_1)+\cdots+(r_n-s_n),\quad r_i-s_i\in R_i$$

由于 0 的表法唯一，知 $r_1=s_1,\cdots,r_n=s_n$.

命题 6　设 $R_i(i=1,\cdots,n)$ 都是环 R 的理想，且 $R=R_1+\cdots+R_n$，那么 $R=\bigoplus_{i=1}^{n} R_i$ 的充分必要条件是

$$R_i\cap\sum_{j\neq i}R_j=\{0\}.$$

证明　若 $a_1\in R_1\cap\sum_{j=2}^{n}R_j$，即

$$a_1=a_2+\cdots+a_n,\quad a_i\in R_i$$

从而有

$$0=(-a_1)+a_2+\cdots+a_n,$$

由表法唯一性得 $a_1=0$，$R_1\cap\sum_{j=2}^{n}R_j=\{0\}$.

反之，若对任意 i 均有 $R_i\cap\sum_{j\neq i}R_j=\{0\}$，且有 $a_i\in R_i$ 使

$$-a_i=a_1+\cdots+a_{i-1}+a_{i+1}+\cdots+a_n,$$

即 $-a_i\cap\sum_{j\neq i}R_j$，从而知 $a_i=0$.

命题 7　对任意一个指标集 I，$R_i(i\in I)$ 为环 R 的理想，且 $R=\sum_{i\in I}R_i$，那么，对任意 $i,j\in I$，$i\neq j$ 及任意 $a\in R_i$，$b\in R_j$ 均

有 $ab=0$.

证明 与 I 为有限集一样，有

$$R_i \cap \sum_{l\neq i} R_l = \{0\},$$

但 $ab \in R_iR_j \in R_i \cap \sum_{l\neq i} R_l$，故 $ab=0$.

习 题

1. 设 p 是个素数，给出 $\mathbf{Z}/(p^2)$ 的所有极大理想.

2. 设 D 是个整环，$I \lhd D$，$I\neq D$. 证明，I 为 D 的素理想的充分必要条件是余集 $D-I$ 在 D 的乘法下封闭.

3. 设 M 为有 1 环 R 的理想，且 $M\neq R$，$R-M$ 的每个元都是单位. 证明，M 是 R 的一个极大理想.

4. 设 R 是个交换的素环，且对每个元 $a\in R$ 恒有一个由 a 决定的整数 $n>1$ 使

$$a^n = a,$$

证明，R 必为除环.

5. 设 R 为一整环，证明 (x) 为 $R[x]$ 的素理想.

6. 设 R_1，R_2 是两个整环. 问：$R_1\oplus R_2$ 是不是整环?

7. 设 F_1，F_2 是两个域，找出 $F_1\oplus F_2$ 的全部理想.

8. 设 R，S 都是环. 若它们都是交换环，则 $R\oplus S$ 也是交换环. 若它们的每个元的加法周期都是有限的，则 $R\oplus S$ 的每个元的加法周期也是有限的. 若它们的每个元都是幂零的，则 $R\oplus S$ 的每个元也都是幂零的.

9*. 设 f 是交换环 R 到交换环 R' 的满同态，证明，若 P 是 R 的素理想且 $\mathrm{Ker}(f)\subseteq P$，则 $f(P)$ 是 R' 的素理想；若 P' 是 R' 的素理想，则 $f^{-1}(P')$ 是 R 的素理想.

第五章　唯一分解整环

结合环理论源于整数理论，但结合环公理系统限制少，概括面大，一般环可能是不交换的，也可能有零因子，这就很难像研究整数一样讨论分解性、可除性问题.

本章及下一章分别讨论两类特殊环，其结构更接近熟悉的一些数集结构. 本章研究由分解问题引起的一些重要环类，下一章研究具有可除性的环类——域.

有了这些更深入的刻画，使得它们在各应用领域更为活跃.

§1　整　除

设 D 是一个整环.

定义 1　设 a，$b\in D$，$b\neq 0$，说元素 b 能整除元素 a，如果有 $c\in D$，使 $a=bc$. 此时，也说 a 能被 b 整除，或说 b 是 a 的一个因子，记为 $b\mid a$，否则就说 b 不能整除 a，记为 $b\nmid a$.

在上一章已经讲过，如果元素 b 是 D 的单位，即 b 在 D 中有逆元，那么 b 可以整除 D 中每一个元素.

例如，整数环中，1 和 -1 都是单位，1 和 -1，2，-2 均能整除 2.

又如，$\mathbf{R}[x]$ 中多项式 $x-\sqrt{2}$ 整除 x^2-2.

例 1　设 F 是个域，那么 $f(x)$ 为 $F[x]$ 的一个单位的充分必要条件是 $f(x)=c$，$c\in F$，$c\neq 0$.

事实上，$f(x)$ 在 $F[x]$ 中有逆元当而且仅当有 $f(x)\in F[x]$

使$f(x)g(x)=1$，当而且仅当$f(x)$为零次多项式，$f(x)=c$，$c\in F$，$c\neq 0$.

定义 2 设a，$b\in D$. 说a，b是相伴的，如果$a|b$且$b|a$.

命题 1 元素a与元素b相伴必要而且只要有D中单位ε，使$b=\varepsilon a$.

事实上，a与b相伴必有C，$D\in D$使

$$ac=b,\qquad bd=a,$$

$$a=bd=acd,$$

进而$cd=1$，c，d为单位.

反之，若ε为D之单位，$b=\varepsilon a$，因而可逆，又必有$a=\varepsilon^{-1}b$，a与b必相伴.

定义 3 对于$a\in D$，所有单位以及与a相伴的元素均称为a的**平凡因子**. D中元素a不是单位，也不为零元，且没有非平凡因子者称为**不可约元或既约元**.

例 2 整数环$\mathbf{Z}$中，素数p的因子只有1，-1，p和$-p$，故p是$\mathbf{Z}$的不可约元.

例 3 域F上的多项式$x-c$ $(c\in F)$是环$F[x]$的一个不可约元.

首先，$x-c$不是零多项式.

其次，$x-c$不是$F[x]$的恒等元，而且若有$f(x)\in F[x]$是$x-c$的因子，可设

$$f(x)g(x)=x-c,$$

那么$f(x)$的次数必为1或为0. 如果$f(x)$次数为0，导致$f(x)=b$，$b\in F$，$b\neq 0$，此时$f(x)$是$F[x]$的单位，$g(x)$与$x-c$相伴；如果$f(x)$次数为1，则$g(x)$为单位，$x-c$与$f(x)$相伴，故多项式$x-c$在$F[x]$中无非平凡因子.

例 4 看$\mathbf{R}[x]$和$\mathbf{Z}[x]$中的多项式x^2-2.

在$\mathbf{R}$上，因为

$$x^2-2=(x+\sqrt{2})(x-\sqrt{2})$$

而 $x+\sqrt{2}$ 既不是 $\mathbf{R}[x]$ 中单位又不是与 x^2-2 相伴的，$x+\sqrt{2}$ 是 x^2-2 的非平凡因子. x^2-2 不是 $\mathbf{R}[x]$ 的不可约元.

在 $\mathbf{Z}$ 上，若有整数 m，n，k，l 使

$$x^2-2=(mx+n)(kx+l),$$

则必有

$$x^2-2=mkx^2+(kn+ml)x+nl.$$

由多项式相等之定义，推出

$$mk=1,\qquad -nl=2,\qquad kn+ml=0,$$

从而 $m=k=\pm 1$. 这样，就导致

$$kn+ml=k(n+l)=0,$$

$$n+l=0,\qquad -nl=2,$$

必有 $n^2=2$. 这是办不到的. 所以，x^2-2 在 $\mathbf{Z}[x]$ 上不能有一次多项式作为其因子.

设 $x^2-2=f(x)g(x)$，则 $f(x)$ 或 $g(x)$ 必有一个次数为 0，为非零常数，也就是 $\mathbf{Z}[x]$ 的单位，另一个必然是和 x^2-2 相伴的.

这说明 x^2-2 在 $\mathbf{Z}[x]$ 中是不可约元.

命题 2 若 p 是 D 的不可约元，ε 是 D 的单位，则 εp 亦为 D 的不可约元.

证明 首先，因为 D 为整环. 由 $p\neq 0$ 及 $\varepsilon\neq 0$ 知 $\varepsilon p\neq 0$.

其次，εp 必不是 D 中单位. 若不然，就有 $a\in D$ 使得 $a(\varepsilon p)=(a\varepsilon)p=e$，推出 p 为单位而导出矛盾.

最后，设 b 是 εp 的一个因子，有 $c\in D$ 使

$$\varepsilon p=bc.$$

由于 ε 是单位，有逆，故 $p=(\varepsilon^{-1}b)c$. 而 p 是不可约元，$\varepsilon^{-1}b$ 只能是单位，或者它是与 p 相伴的. 当 $\varepsilon^{-1}b$ 是单位时，b 必为

单位；当 $\varepsilon^{-1}b$ 与 p 相伴时，有单位 $\delta\in D$ 使

$$\delta\varepsilon^{-1}b = p,$$

$\delta\varepsilon^{-1}$ 仍为单位，b 是与 p 相伴的. 这说明 b 一定是 p 的一个平凡因子.

即 εp 无非平凡因子，εp 是不可约元.

命题 3 设 D 中元 a 非零，且

$$a = bc, \quad b, c \in D.$$

那么 b 为 a 的非平凡因子的充分必要条件是 c 为 a 的非平凡因子.

证明 如果 c 为 a 的平凡因子. 当 c 为单位时，b 是和 a 相伴的；当 c 是和 a 相伴的元素时，$c=\varepsilon a$，ε 为单位，于是

$$a = bc = \varepsilon ba,$$

而 $a\neq 0$，D 无非零的零因子，故 $\varepsilon b=e$，b 是单位. 也就是说，c 是平凡因子时，b 亦是平凡因子.

定义 4 满足下列条件的整环 D 称为**唯一分解整环**：

(1) 如果 $a\in D$，$a\neq 0$，a 不是单位，那么 a 必可以写成若干个 D 的不可约元的乘积，即

$$a = p_1p_2\cdots p_s, \quad p_i \text{ 是 } D \text{ 的不可约元.}$$

(2) 如果 $a\in D$，且

$$a = p_1p_2\cdots p_s = q_1q_2\cdots q_t,$$

其中 p_i 和 q_j 都是 D 的不可约元，那么 $s=t$，并且适当调整 q_j 的顺序后，可使 q_j 与 p_j 恰好是对应相伴的，$j=1, 2, \cdots, t$.

这个定义之条件(1)对单位和零元不做要求，这是很自然的，因为在任何整环中，若

$$0 = a_1a_2\cdots a_s$$

则必有 i 使 $a_i=0$，故 a_j 不能都是不可约元.

同样，若 ε 为 D 的单位，且

$$\varepsilon = a_1a_2\cdots a_s,$$

则每个 a_j 都是单位，都不是不可约元.

例如，整数环是唯一分解整环，每个非 0 又不为 1 或 -1 的整数 m，均有

$$m = p_1^{\sigma_1}p_2^{\sigma_2}\cdots p_t^{\sigma_t},$$

其中 p_i 为素数. $a_i > 1$. 而且，如果不计顺序，上述分解表达式是唯一的(可以差正负号).

又如，实多项式环 $\mathbf{R}[x]$ 是个唯一分解整环. 当实多项式 $f(x)$ 为非零非单位，即不是常数多项式时，必有

$$f(x) = p_1(x)^{\sigma_1}\cdots p_t(x)^{\sigma_t},\quad a_i > 1, \tag{1}$$

其中每个 $p_i(x)$ 都是实的不可约多项式. 实数域上不可约多项式必为一次式或二次多项式.

这种分解，如果不计因式顺序，是唯一的(相应因式可相差一非零常数倍).

而复数域上多项式环 $\mathbf{C}[x]$ 的不可约元即不可约多项式必为一次式，每个非常数多项式 $f(x)$ 亦能表成以上(1)的形式，只不过诸 $p_i(x)$ 均为一次多项式. $\mathbf{C}[x]$ 也是唯一分解整环.

例 5　看复数环 $\mathbf{C}$ 的子环

$$\langle \mathbf{Z} \cup \{\sqrt{-5}\} \rangle = \{A + B\sqrt{-5} \mid a, b \in \mathbf{Z}\}.$$

它含 1，故为整环，记为 D.

为说明它不是唯一分解整环，建立映射

$$\varphi: a + b\sqrt{-5} \to a^2 + 5b^2,$$

这是 D 到整数环 $\mathbf{Z}$ 的一个映射，即规定每个元素对应自己的模数的平方.

可以看出，对任意 $z, \omega \in D$，有

(1) $\varphi(z) \geqslant 0$,

(2) $\varphi(z) = 0$ 当而且仅当 $z = 0$,

(3) $\varphi(z\omega) = \varphi(z)\varphi(\omega)$.

我们仅验证一下条件(3)，设

$$z = a + b\sqrt{-5}, \qquad \omega = c + d\sqrt{-5},$$

其中 a, b, c, d 均为整数. 于是

$$\varphi(z) = a^2 + 5b^2, \qquad \varphi(\omega) = c^2 + 5d^2.$$

再由

$$\begin{aligned} z\omega &= (a + b\sqrt{-5})(c + d\sqrt{-5}) \\ &= ac + (-5bd) + (ad + bc)\sqrt{-5} \end{aligned}$$

得

$$\begin{aligned} \varphi(z\omega) &= (ac - 5bd)^2 + 5(ad + bc)^2 \\ &= (ac)^2 + 5(ad)^2 + 5(bc)^2 + 25(bd)^2 \\ &= (a^2 + 5b^2)(c^2 + 5d^2) \\ &= \varphi(z)\varphi(\omega). \end{aligned}$$

现在来决定 D 中的单位. 若 $z\omega = 1$, 那么

$$\varphi(z)\varphi(\omega) = \varphi(1) = 1.$$

而 $\varphi(z)$ 和 $\varphi(\omega)$ 都是整数, 又非负, 故

$$\varphi(z) = 1, \qquad \varphi(\omega) = 1.$$

设 $z = a + b\sqrt{-5}$. 再由

$$\varphi(3) = 1 = a^2 + 5b^2$$

知 $b = 0$, $a = \pm 1$. 也就是说, D 中单位只有 1 和 -1.

D 中元素 x 仅仅与自己, 与 $-x$ 是相伴的.

观察 $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, 其中 9, 3, $2 + \sqrt{-5}$ 和 $2 - \sqrt{-5}$ 都是 D 中元素, 而 3 和 $2 + \sqrt{-5}$ 和 $2 - \sqrt{-5}$ 都不是相伴的.

剩下来, 我们只需证明 3 和 $2 + \sqrt{-5}$ 都是 D 的不可约元. 设有 $z, \omega \in D$ 使 $3 = z\omega$. 那么

$$\varphi(z\omega) = \varphi(3) = 9 = \varphi(z)\varphi(\omega).$$

$\varphi(z)$ 只能是 1, 3 或者 9. 若 $\varphi(z) = 1$, 它是单位; 若 $\varphi(z) = 9$, 则 $\varphi(\omega) = 1$, ω 是单位, z 与 3 是相伴的. 两种情形下, z 都不

是整数 3 的非平凡因子.

要想使 3 有非平凡因子，只能是

$$\varphi(z) = a^2 + 5b^2 = 3, \quad a, b \in \mathbf{Z}.$$

但这是不能可能的. 这说明 3 是整环 D 中的不可约元.

同样，由于 $\varphi(2+\sqrt{-5}) = 9$，若有 $z, \omega \in D$ 使 $z\omega = 2+\sqrt{-5}$，则必有

$$\varphi(z)\varphi(\omega) = \varphi(2 + c3) = 9.$$

$\varphi(z)$ 只能是 1 或 9，z 只能是单位或是与 $2+\sqrt{-5}$ 相伴的.

$2+\sqrt{-5}$ 和 $2-\sqrt{-5}$ 也是 D 的不可约元.

定理 1 设 D 是个唯一分解整环，p 是个不可约元. 如果 $p\mid(ab)$，那么 $p\mid a$ 或 $p\mid b$.

证明 如果 $p\mid ab$，设有 $c\in D$ 使 $ab = pc$.

当 a, b 均不为 0，也不是 D 中单位时，c 必不为 0. 而且 c 也不能是单位，否则，必有

$$p = (c^{-1}a)b.$$

而 p 是素元，上式导致 $c^{-1}a$ 为单位. 同时，只要 $c^{-1}a$ 为单位则 a 亦为单位，矛盾.

这样，由于 c 不是 0 也不是单位，而 D 是唯一分解整环，必有

$$c = p_1p_2\cdots p_n,$$

其中每个 p_i 都是 D 的不可约元. 于是

$$ab = pp_1\cdots p_n,$$

就是元素 ab 的一个不可约因子分解式.

但 a, b 均不为 0 又不为单位，它们可单独分解为

$$a = q_1q_2\cdots q_m, \qquad b = r_1r_2\cdots r_t,$$

其中 q_j 和 r_k 也都是 D 的不可约元. 于是，我们得到

$$ab = q_1\cdots q_mr_1\cdots r_t = pp_1p_2\cdots p_n,$$

据唯一分解整环的定义，不可约元 q_1，…，q_m，r_1，…，r_t 中必然有一个与 p 是相伴的.

如果 q_j 是与 p 相伴的，由 $q_j|a$ 可推知 $p|a$；如果 r_k 是与 p 相伴的，由 $r_k|b$ 可推出 $p|b$.

当 $a=0$ 时，当然有 $p|a$. 即任意不可约元 p 都满足定理要求.

当 a 为单位时，$ab=cp$ 蕴涵 $b=(a^{-1}c)p$，也就是 $p|b$.

所以，当 a 和 b 有一个为 0 或有一个为单位时，定理恒对.

定理 1 引起我们讨论另一个重要概念.

定义 5 设 D 是个整环，$p\in D$. 若 p 不是零元也不是单位，且对任意 a，$b\in D$，只要 $p|ab$，那么必有 $p|a$ 或者 $p|b$，则说 p 是 D 的一个**素元**.

从定义中可以看出，对任意整环 D 来说，它的素元 p 一定是不可约的. 因为，若

$$p = ab,\quad a,b\in D,$$

当然有 $p|ab$，由 p 的素性，必有 $p|a$ 或 $p|b$. 如果 $p|a$，则 a 与 p 是相伴的，b 为单位；如果 $p|b$，则 b 与 p 是相伴的，a 为单位. 从而 p 不能有非平凡的因子.

定理 1 指明，对于唯一分解整环，p 是不可约元则一定是素元.

那么，对于一般的一个整环，素元和不可约元是否是同一概念呢？仔细研究上面的例 5 即可说明问题. 在整环 $D=\langle \mathbf{Z}\cup\{\sqrt{-5}\}\rangle$ 中，3 是个不可约元，3 能整除 9，且

$$9=(2+\sqrt{-5})(2-\sqrt{-5}).$$

但 $2+\sqrt{-5}$ 和 $2-\sqrt{-5}$ 都是 D 的不可约元，且它们都不是和 3 相伴的，所以

$$3\nmid(2+\sqrt{-5}),\qquad 3\nmid(2-\sqrt{-5}).$$

这说明 3 是不可约元但不是素元.

由于整数环和域上多项式环都是唯一分解整环，素元与不可约元一致，人们也把素数称为不可约数，把不可约多项式称为素多项式.

我们在处理唯一分解整环的整除性问题时，对不可约元和素元就不必区别了.

定义 6　设 D 是个整环，$a_1, \cdots, a_n \in D$. 如果 $c \in D$，c 整除 $a_1, \cdots, a_n$ 的每一个，则说 c 是元素 $a_1, \cdots, a_n$ 的一个**公因子**.

元素 $d \in D$ 称为元素 $a_1, \cdots, a_n$ 的一个**最大公因子**，如果

(1) d 是 $a_1, \cdots, a_n$ 的一个公因子，

(2) 对任意 $c \in D$，只要 c 是 $a_1, \cdots, a_n$ 的一个公因子，则必有 $c \mid d$.

当一个单位是 $a_1, a_2, \cdots, a_n$ 的一个最大公因子时，则说它们是**互素的**.

定理 2　设 D 是唯一分解整环. 那么不全为 0 的元素 a，b 必有最大公因子. 且各最大公因子都是相伴的.

证明　当 $a=0$ 时，必有 $b=0$，b 就是 a 和 b 的最大公因子；当 $b=0$ 时，a 就是 a，b 的最大公因子.

当 a 为单位时，a 就是 a，b 的最大公因子；当 b 为单位时，b 就是 a，b 的最大公因子.

故，不妨设 a 和 b 都不是 0，也都不是单位. 于是，可设

$$a = p_1 p_2 \cdots p_s, \qquad b = q_1 q_2 \cdots q_t.$$

其中 p_i 和 q_j 都是 D 的素元. 我们先将 a 的诸因子 p_i 中相伴的元素合在一起，写成

$$a = \varepsilon p_1^{l_1} p_2^{l_2} \cdots p_n^{l_n}, \quad l_i \geq 1.$$

ε 是单位. 再把 b 的诸因子 q_j 中与 $p_1, \cdots, p_n$ 相伴的合在一起，写在前面，其余因子列后，即

$$b = \delta p_1^{k_1} \cdots p_n^{k_n} q_1 \cdots q_k,$$

其中 δ 是 D 中单位，$k_j \geqslant 0$（当 p_j 不是 b 的非平凡因子时，$k_j = 0$），q_j 不是 a 的非平凡因子，与任意 p_i 都不是相伴的.

用 $\min\{k, l\}$ 代表自然数 k, l 之最小者，令

$$s_j = \min\{k_j, l_j\}, \quad 1 \leqslant j \leqslant n.$$

可以断言，$d = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$ 就是 a, b 的一个最大公因子.

进一步，设 c 是 a, b 的任意一个公因子. 若 c 是个单位，自然有 $c|d$. 若 c 不是单位，设

$$c = r_1 \cdots r_m, \quad r_i \text{ 是素元},$$

那么，由 $c|a$, $r_i|a$ 知，每个 r_i 必然是与某个 p_j 相伴的，把相伴的元素合在一起，

$$c = \rho p_1^{h_1} p_2^{h_2} \cdots p_n^{h_n}, \quad h_k \geqslant 0.$$

再由 $c|a$，即

$$a = \varepsilon p_1^{l_1} \cdots p_n^{l_n} = f(\rho p_1^{h_1} p_2^{h_2} \cdots p_n^{h_n})$$

可知 $h_1 \leqslant l_1$，否则（即 $l_1 < h_1$），用消去律，得

$$\varepsilon p_2^{l_2} \cdots p_n^{l_n} = f\rho p_1^{h_1 - l_1} \cdots p_n^{h_n}, \quad h_1 - l_1 > 0,$$

必有 $p_1 | p_2^{l_2} \cdots p_n^{l_n}$，与诸 p_i 之为相伴的假设相矛盾. 同理，$h_2 \leqslant l_2$, …, $h_n \leqslant l_n$. 又同理，

$$h_1 \leqslant k_2, \ h_2 \leqslant k_2, \ \cdots, \ h_n \leqslant k_n.$$

也就是 $h_i \leqslant s_i = \min\{l_i, k_i\}$，从而必有 $c|d$，d 是 a, b 的一个最大公因子.

设 d^* 也是 a, b 的一个最大公因子. 因为 d 是个公因子，故 $d|d^*$. 而我们已经证明了 d 是最大公因子，又必有 $d^*|d$，即 d^* 是和 d 相伴的.

每个最大公因子都是和 d 相伴的，从而它们都是相伴的.

推论 设 D 是个唯一分解整环. 那么任意 n 个不全为 0 的元素 $a_1, a_2, \cdots, a_n$ 必有最大公因子.

例题 1 设 D 是个唯一分解整环，a, b 不全是 0，d 是它们

的一个最大公因子. 那么, 对于 D 中任意非零元 c, cd 恰为 ac, bc 的一个最大公因子.

解　读者可以试用定理 2 的证明中使用的方法, 将 a, b, c 写成素元连乘积, 然后求出 ac 和 bc 的最大公因子.

这里用另一种方法证明. 由于 ca, cb 不全为 0, 它们必有最大公因子, 设 f 是它们的一个最大公因子. 首先, d 是 a, b 的公因子, $d \mid a$, $d \mid b$, 故

$$cd \mid ca, \qquad cd \mid cb,$$

即 cd 是 ca 和 cb 的一个公因子. 据 f 的定义, $cd \mid f$.

于是, 可设有 $x \in D$, $f = cdx$.

其次, f 是 ac 的因子, 又是 bc 的因子, 必有 r, $s \in D$ 使

$$ac = fr, \qquad bc = fs,$$

$$ac = cdxr, \qquad bc = cdxs.$$

因为 c 不为 0, 用消去律, 得

$$a = dxr, \qquad b = dxs.$$

这说明 dx 是 a 和 b 的公因子. 由 d 的定义知, $dx \mid d$. 从而 d 与 dx 是相伴的, x 是个单位.

最后, 由 $f = cdx$ 知 f 和 cd 是相伴的.

例题 2　设 D 是个整环, 而且

(1) 如果 $a \in D$, $a \neq 0$, a 不是单位, 那么, a 必可写成若干个 D 的不可约元的乘积, 即

$$a = p_1 p_2 \cdots p_s, \quad p_i \text{ 是 } D \text{ 的不可约元}.$$

(2) 对于 D 的任意不可约元 p, $p(ab)$ 蕴涵 $p \mid a$ 或 $p \mid b$.

则 D 必为唯一分解整环.

分析　按着唯一分解整环定义要求, 只需证明分解表达式的唯一性. 设

$$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t, \qquad (*)$$

其中 p_i 和 q_j 都是不可约元, 需证明 $s = t$, 适当调整顺序后, p_i

是与 q_j 相伴的.

条件(2)表面上是 $p\mid ab$ 则 $p\mid a$ 或 $p\mid b$，实际上蕴涵着 $p\mid a_1a_2\cdots a_n$，则 p 必然整除 a_i 中的一个.

因此，我们可以对(*)式左端之 s 用数学归纳法.

解　设在 D 中有不可约元 p_i，q_j，$i=1$，…，s；$j=1$，…，t 使

$$p_1p_2\cdots p_s = q_1q_2\cdots q_t \qquad (*)$$

成立. 我们对 s 用数学归纳法来证明必有 $s=t$ 且调整顺序后 p_i 和 q_i 是相伴的，$i=1$，2，…，s.

当 $s=1$ 时，

$$p_1 = q_1\cdots q_t = q_1(q_2\cdots q_t),$$

由于 p_1 是素元，故 q_1 或为单位或是与 p_1 相伴的. 但 q_1 也是不可约元，不为单位，所以 q_1 必然是与 p_1 相伴的.

p_1 和 q_1 是相伴的，如果 $t\geqslant 2$，那么 $q_2\cdots q_t$ 必为单位，而 $q_2\cdots q_t$都是不可约元，这是不可能的. 从而只有 $s=t=1$ 才行. 命题当 $s=1$ 时得证.

现假定命题对 $s-1$ 情形是对的. 那么

$$p_1p_2\cdots p_s = q_1q_2\cdots q_t \qquad (*)$$

意味着 p_1 必整除 q_1，…，q_t 之一，因为允许适当调整顺序，我们不妨假定 $p_1\mid q_1$.

由于 q_1 也是不可约元，p_1 又不是单位，从而 p_1 是与 q_1 相伴的. 设 $q_1=\varepsilon p_1$，ε 是单位. 于是(*)变成

$$p_1p_2\cdots p_s = q_1\varepsilon q_2\cdots q_t.$$

$p_1\neq 0$，可用消去律，得

$$p_2\cdots p_s = q_2'q_3\cdots q_t, \qquad (**)$$

其中 $q_2'=\varepsilon q_2$ 仍然是不可约元.

注意，(* *)式之左端为 $s-1$ 个不可约元之积，右端是若干个不可约元之积，按归纳法假定，必然有 $s-1=t-1$，即

$s=t$而且调整 q_j 的顺序后，p_2 和 q_2' 是相伴的，p_s 是和 q_s 相伴的，…，p_s 是和 q_s 相伴的.

由于 q_2' 与 q_2 相伴，故 p_2 与 q_2 是相伴的. 归纳法完成.

例题 3　研究有理数环 **Q** 的子集

$$R = \{a/b \in \mathbf{Q} \mid b \text{ 为奇数}\}.$$

(1) R 对有理数减法和乘法封闭，R 是 **Q** 的子环，$1=1/1 \in R$. R 是个整环.

(2) 任取 $a/b \in R$，如果 $c/d \in R$ 使

$$(a/b) \cdot (c/d) = 1,$$

即 $ac=bd$，由于 b 和 d 都是奇数，从而 a 必为奇数.

反过来，若 $a/b \in R$，a 为奇数，必有

$$(a/b) \cdot (b/a) = 1,$$

即 a/b 是 R 的单位.

所以，R 中元素 a/b 为单位的充要条件是 a 为奇数.

(3) 如果有 a/b，$c/d \in R$ 使

$$(a/b) \cdot (c/d) = 2 = 2/1,$$

则 $ac=2bd$，2 必整除 a 或整除 c. 若设 $a=2f$，那么由

$$fc = bd$$

可知 f 必为奇数，$a/b=2\cdot(f/b)$. 这说明 a/b 是和 2 相伴的. 若 2 整除 c，则 a 奇数，a/b 必然是个单位.

所以，2 没有非平凡因子，2 是环 R 的一个不可约元.

(4) 任取 $a/b \in R$，若它不是 0 也不是单位，即 a 不为 0 也不为奇数，可设 $a=2^t d$，d 是个奇数. 于是

$$a/b = (d/b) \cdot 2)2 \cdot \cdots \cdot 2, \quad t \text{ 个 } 2,$$

其中 $d/b\cdot 2$ 和 2 都是 R 的不可约元，a/b 已写成不可约元的连乘积形式.

(5) 任取 $a/b \in R$，如果 $4 \mid a$，$a=4c$，那么

$$a/b = 2 \cdot (2c/b).$$

说明，2 是 a/b 的因子且不是和 a/b 相伴的，即 2 是 a/b 的非平凡因子. a/b 不是不可约元，这说明，a 为奇数时，a/b 是 R 的单位，$4\mid a$ 时，a/b 不是不可约元.

所以，R 的所有不可约元都是和 2 相伴的.

(6) 我们用 $\parallel$ 代表环 R 中的整除符号，以区别本题前面用的整数的整除符号 $\mid$.

设 a/b, $c/d\in R$,

$$2\parallel[(a/b)\cdot(c/d)],$$

即有 $f/h\in R$，使 $(a/b)\cdot(c/d)=2\cdot(f/h)$，也就是

$$2fbd = ach.$$

由于 h 是奇数，2 不能(整数的)整除 h，从而 $2\mid a$ 或 $2\mid c$. 即

$$2\parallel(a/b) \text{ 或 } 2\parallel(c/d),$$

由上题可知 R 是唯一分解整环.

习　题

1. 在整环 $\mathbf{Z}_5[x]$ 中找出所有单位，给出 $2x^3+x$ 的所有相伴元.

2. 证明：在整环 $\mathbf{Z}_2[x]$ 中，x^3+x+1 是不可约元.

3. 复数环 $\mathbf{C}$ 中由整数集 $\mathbf{Z}$ 和 $\sqrt{-2}$ 生成的子环，记为 $\mathbf{Z}[\sqrt{-2}]$. 问 5 在 $\mathbf{Z}[\sqrt{-2}]$ 中是不是不可约元素.

4. 设 F 是个域，a, $b\in F$. 证明：在 $F[x]$ 中，$x-a$ 与 $x-b$ 互素的充分必要条件是 $a\neq b$.

5. 设 D 是个唯一分解整环，a, $b\in D$. 那么 a, b 互素的充分必要条件是它们不含相同的素元因子.

6. 设 D 是个整环，把元素之间的整除看成是 D 上的一个关系. 证明：如果整除关系在 D 的非零元素 $D^*=D-\{0\}$ 上是个等价关系，那么 D 必然是个域.

7. 设 x, y 是整环 D 的元素. 证明：

(a) $x|y$ 的充分必要条件是 $(x) \supseteq (y)$；

(b) x 和 y 相伴的充分必要条件是 $(x) = (y)$；

(c) y 是 x 的非平凡因子的充分必要条件是 $(x) \subset (y) \subset D$.

§2　主理想整环和欧氏环

要像上节例题 2 那样给出更多的环为唯一分解整环的充分必要条件当然是很有意义的事情. 同时，为了应用方便，也需要得到一些环为唯一分解整环的充分条件，本节介绍其中两种.

定义 1　如果整环 D 的每个理想都是主理想，则说 D 为主理想整环.

例如，整数环 $\mathbf{Z}$ 是个主理想整环.

第四章 §4 定理 2 证明了域 F 上的多项式环 $F[x]$ 是个主理想整环.

例 1　看上节例题 3 中的

$$R = \{a/b \in \mathbf{Q} \mid b \text{ 为奇数}\}.$$

设 N 是 R 的一个理想. 当 $N = \{0\}$ 时 N 恰为零元 0 生成的主理想 (0).

当 $N \neq \{0\}$ 时. 对任意 $a/b \in N$, 设

$$a/b = 2^t(c/b), \ c \text{ 为奇数}, \ t \geqslant 0.$$

可以证明，非负整数 t 是由元素 a/b 完全确定的.

设 $a/b = e/f$, 其中 b 和 f 都是奇数. 由 $af = be$ 及整数的唯一分解定理，e 和 a 必含相同个 2 的因子，都是 t 个. 故

$$e/f = 2^t(h/f),$$

h 和 f 都是奇数. 这说明，t 与 a/b 表达中元素选择无关.

建立映射

$$\varphi: a/b \to t, \quad a/b = 2^t(c/b), \quad c\text{ 为奇数}.$$

这是环 N 到整环 $\mathbf{Z}$ 的一个映射.

由于 $\mathrm{Img}(\varphi)$ 是个非负整数的集合，它必有最小元，设为 n. 既然 $n \in \mathrm{Img}(\varphi)$，那么必有 R 的元素 g/d 使得

$$\varphi(g/d) = n, \quad g/d = 2^n(l/d), \quad l\text{ 为奇数}. \qquad (*)$$

现在，我们任取 $a/b \in N$，由 n 的定义，必有

$$n = \varphi(g/d) \leqslant \varphi(a/b) = t,$$

其中 $a/b = 2^t(c/b)$，c 是个奇数. 故

$$a/b = 2^t(c/b) = 2^n(l/d) \cdot (d/l) \cdot 2^{t-n}(c/b),$$

其中 $t-n \geqslant 0$，$2^{t-n}(c/b) \in R$. 从而 $2n(l/d) = g/d$ 在 R 整除 a/b，即

$$a/b \in (g/d),\ N = (g/d).$$

这说明 R 的每个理想都是主理想.

命题 1 设 D 是个主理想整环. 那么，在 D 中不能有这样无穷多个理想 $N_1, N_2, \cdots$，使

$$N_i \subseteq N_{i+1}, \quad N_i \neq N_{i+1}, \quad i = 1, 2, \cdots$$

证明 用反证法. 若有无穷多个理想 $N_i(i=1, 2, \cdots)$ 使得 $N_i \subseteq N_{i+1}$，且 $N_i \neq N_{i+1}$，令 $N = \bigcup_i N_i$，可以证明它亦为 D 的一个理想.

首先，对任意 $x, y \in N$，据并集 N 的定义，x, y 必分别属于某个 N_i 和 N_j，即

$$x \in N_i, \qquad y \in N_j.$$

在 i 和 j 两个自然数中不妨设 $i \leqslant j$，于是由诸 N_t 前面包含关系知 $N_i \subseteq N_j$. 从而有

$$x \in N_i \subseteq N_j, \qquad y \in N_j.$$

但是，已知 N_j 是 D 的理想，故 $x-y \in N_j$，进一步，$x-y \in N_j \subseteq N$. N 对减法封闭.

其次，对任意 $r\in D$，$x\in N$. 设 $x\in N_i$，那么，由于 N_i 是 D 的理想，必有 rx，$xr\in N_i$. 从而 rx，$xr\in N_i\subseteq N$.

所以，N 为 D 的一个理想.

D 为主理想环，设 $N=(x)$. 而据 N 的定义，$x\in N$，则 x 必属于某个 N_i. 进而 (x) 的所有元素都应属于 N_i，对于这个 i，有

$$N_{i+1}\subseteq N=(x)\subseteq N_i\subseteq N_{i+1},$$

也就是 $N_i=N_{i+1}$. 与假定相矛盾.

命题 2　设 D 是个主理想整环，$p\in D$，$p\neq 0$. 那么，下列说法等价：

(1) p 是 D 的一个素元；

(2) (p) 是 D 的一个极大理想；

(3) (p) 是 D 的一个素理想.

证明　用循环证法. 如果 p 是 D 的素元，那么 p 不是单位，故

$$1\notin(p)=\{rp\in D\mid r\in D\}.$$

所以，$(p)\neq D$.

设 N 是 D 的理想，$(p)\subseteq N$，$(p)\neq N$. 由于 D 是主理想环，可设 $N=(a)$，$a\in D$. 于是，$p\in N$ 意味着有 $b\in D$ 使 $p=ab$.

又由于 p 是素元，a 必为单位或者是与 p 相伴的. 如果 a 是和 p 相伴的，则必有 $a\in(p)$，从而 $(a)=N=(p)$，与假设矛盾. 故，a 只能是个单位，而单位生成的理想就是 D 本身. 所以 $N=D$. (p) 是个极大理想.

这样，我们由条件(1)推出了条件(2).

下面，由(2)推(3). 设 (p) 是极大理想. 由第五章 §2 知乘余环 $D/(p)$ 是个域，任取 a，$b\in D$，如果 $ab\in(p)$，那么在 $D/(p)$ 中

$$ab+p=[a+(p)][b+(p)]=p,$$

其中 p 乃是 $D/(p)$ 的零元. 而域当然不含非零的零因子，故

$a+(p)=(p)$或$b+(p)=(p)$，也就是$a\in(p)$或$b\in(p)$．(p)是D的素理想．

最后，由(3)来推(1)．设(p)是个素理想．如果有$a,b\in D$使$ab=p$．那么$ab\in p$，于是必有$a\in(p)$或$b\in(p)$．

若$a\in(p)$，则$p|a$，从而a是和p相伴的，b为D的一个单位．若$b\in(p)$，则b是与p相伴的，a是D的一个单位．总之，p没有任何非平凡因子．又因为$(p)\neq D$，p不是D的单位，同时$p\neq 0$，故p为D之素元．

定理 1 每个主理想整环D都是唯一分解整环．

证明 现先来证明当D为主理想整环时，它的非0非单位的元素必为若干素元之积．

若不然，设$a\in D$，$a\neq 0$，a不是单位，且a不能写成若干个素元之乘积．那么：

首先，a必然不是素元，否则$a=a$即为素元积形式．于是a必然仅有非平凡的因子，设b和c是a的非平凡因子，$a=bc$．于是

$$a\in(b),\qquad a\in(c).$$

并且，由于b和c均不是和a相伴的，必有

$$b\notin(a),\qquad c\notin(a).$$

从而有

$$(a)\subseteq(b),\quad (a)\neq(b),$$
$$(a)\subseteq(c),\quad (a)\neq(c).$$

其次，由$a=bc$，而a不是素元连乘积，可以断言b或c必然至少有一个也不是素元连乘积（当b和c均为素元乘积时，$bc=a$就是素元之积），取这样一个不是素元乘积者记为a_1，它满足

(1) a_1是a的非平凡因子，$(a)\subseteq(a_1)$，$(a)\neq(a_1)$；

(2) a_1不能写成素元之连乘积形式．

由(1)可知 a_1 非 0 非单位，由(2)进一步知道 a_1 具有和 a 完全一样的性质.

最后，我们完成仿照对 a 的讨论，可找到 $a_2 \in D$，$(a_2) \subseteq (a_1)$，$(a_2) \neq (a_1)$ 且 a_2 不是素元之积. 这样不断做下去，即有

$$(a) \subseteq (a_1) \subseteq \cdots, \quad (a_i) \neq (a_{i+1}), \quad i = 1, 2, \cdots.$$

而命题 1 已经证明了，在主理想整环里是不能有这种结论的. 这表明对 a 的假定不能成立.

再来证明 D 有分解的唯一性. 设

$$p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t, \qquad (*)$$

其中 p_i 和 q_j 都是 D 的素元. p_1 是素元，由命题 2 知，(p_1) 是 D 的一个素理想. $(*)$ 表明，

$$q_1 q_2 \cdots q_t \in (p_1),$$

故必有某个 $q_l \in (p_1)$，因为顺序可以考虑，我们不妨假设 $q_1 \in (p_1)$，即 $p_1 | q_1$. 但 q_1 是素元，p_1 是 q_1 的因子，p_1 必然是与 q_1 相伴的，

$$p_1 = \varepsilon q_1, \quad \varepsilon \text{ 是单位}.$$

将 $(*)$ 中 p_1 消去，得

$$p_2 \cdots p_s = (\varepsilon q_2) \cdots q_t,$$

其中 εq_2 也是素元.

继续下去不并不断调整右端素元顺序，即有 p_i 和 q_i 是相伴的，对所有 $i = 1, 2, \cdots, t$ 都成立，同时 $s = t$.

例题 1　设 D 是个主理想整环，其元素 a，b 不全为 0. 那么，必有 $m, n \in D$ 使得 $d = ma + nb$ 恰好是 a，b 是一个最大公因子.

解　看 D 中由子集 $\{a, b\}$ 生成的理想 N. 由于 D 有 1 且可交换，N 中每个元 r 必可写成

$$r = xa + yb, \quad x, y \in D.$$

另一方面，D 是主理想环，必有 $d \in D$ 使 $N = (d)$. 设 $d = ma +$

nb，我们来证明 d 是 a 和 b 的一个最大公因子.

首先，$a\in N=(d)$，$a=cd$，$d\mid a$. 同样，$b\in(d)$，$d\mid b$. 所以，d 是 a，b 的一个公因子.

其次，假设 f 是 a，b 的公因子，由 $f\mid a$ 和 $f\mid b$ 立知 $f\mid(ma+nb)$，即 $f\mid d$.

所以，d 是 a 和 b 的一个最大公因子.

现在再介绍整环为唯一分解整环的另一个判别方法.

定义 2　整环 D 称为**欧氏环**，如果有由 D 之所有非 0 元集合 D_0 到正整数集 $\mathbf{N}^*$ 的映射 d 满足

(1) 如果 a，$b\in D_0$ 且 $a\mid b$，则 $d(a)\leqslant d(b)$；

(2) 如果 $a\in D$，$b\in D_0$，则必有 q，$r\in D$ 使 $a=bq+r$，$d(r)<d(b)$ 或 $r=0$.

例如，整数环 $\mathbf{Z}$ 上规定每个数对应其绝对值

$$d(r)=|r|,\quad r\in D$$

利用整数的长除法，即知 $\mathbf{Z}$ 即为一个欧氏环.

又如，对任意域 F，规定

$$d: f(x)\to \deg f(x),\quad f(x)\in F[x],\quad f(x)\neq 0,$$

即得所有非 0 多项式集 $F[x]_0$ 到非负整数集 $\mathbf{N}^*$ 的一个映射.

在第五章 §4 定理 1 中，我们证明了，对任意 $f(x)\in F[x]$，$g(x)\in F[x]_0$，必有 $q(x)$，$r(x)\in F[x]$ 使得

$$f(x)=g(x)q(x)+r(x),$$
$$\deg r(x)<\deg g(x).$$

由于原来规定了零多项式的次数为 $-\infty$，那里的

$$\deg r(x)<\deg g(x)$$

就包含了两种情形，$r(x)$ 为 0，或者

$$0\leqslant \deg r(x)<\deg g(x).$$

这与欧氏环定义的要求完全一致. 故 $F[x]$ 是个欧氏环.

命题 3　设 D 对映射 d 是个欧氏环，$a\in D$，$a\neq 0$. 那么，a

为单位的充分必要条件是 $d(a)=d(1)$.

证明　如果 a 是 D 的一个单位，即有 c 使 $ac=1$，则

$$
\begin{aligned}
d(a) &\leqslant d(ac) && (\text{定义 } 2)\\
&= d(1) && (ac=1)\\
&\leqslant d(1\cdot a) && (\text{定义 } 2)\\
&= d(a), && (1\text{ 的性质})
\end{aligned}
$$

也就是 $d(a)\leqslant d(1)\leqslant d(a)$，$d(a)=d(1)$.

反之，如果 $d(a)=d(1)$，由于有

$$1 = aq + r,\quad r = 0 \text{ 或 } d(r) < d(a),$$

而

$$d(r) < d(a) = d(1) \leqslant d(1\cdot r) = d(r)$$

是不可能的，故必有 $r=0$，$1=aq$，a 为 D 的单位.

定理 2　每个欧氏环都是主理想整环.

证明　设整环 D 对映射 d 是个欧氏环，A 是 D 的一个理想.

如果 $A=\{0\}$，那么，它就是 0 生成的主理想.

如果 $A\neq\{0\}$，它包含非 0 元素，令

$$T = \{d(x) \in \mathbf{N}^* \mid x \in A\}.$$

T 是 A 在映射 d 之下的象. 由于 A 有非 0 元，所以 T 是个非空的非负整数集，它必有最小的元. 设 $a\in A$ 使得 $d(a)$ 是 T 的最小元.

我们断言，$A=(a)$.

$a\in A$，显然有 $(a)\subseteq A$. 任取 $x\in A$，据定义，必有 $q, r\in D$ 使

$$x = aq + r,\qquad r = 0 \text{ 或 } d(r) < d(a).$$

但是，A 是 D 的理想，由 $x, a\in A$ 可知 $aq\in A$ 而且

$$x - aq = r \in A.$$

而 $d(r)<d(a)$ 与 a 的选取相矛盾，故只能 $r=0$，也就是 $x=$

aq, $x \in (a)$. 由 x 的任意性推出 $A \subseteq (a)$.

总之, $A = (a)$, A 是个主理想.

这样, 我们得到下列环类的关系:

欧氏环类 $\subseteq$ 主理想整环类 $\subseteq$ 唯一分解整环类 $\subseteq$ 整环类.

至于各类之间是否真的不同, 也就是给出些具体例子说明, 有的主理想整环不是欧氏环, 有的唯一分解整环不是主理想整环, 等等, 也并非难事. 但, 这些例子不是初学者十分熟悉的, 这里就不予介绍了.

对于欧氏环, 讨论其整除性, 我们有

命题4 设 D 对映射 d 为欧氏环, $b \neq 0$, $a \mid b$ 且 a 不是单位也不是和 b 相伴的. 则 $d(a) < d(b)$.

证明 据定义, 应有 q, $r \in D$ 使

$$a = bq + r, \qquad r = 0 \text{ 或 } d(r) < d(b).$$

但, $r = 0$ 则意味着 $b \mid a$, 导致 a 是和 b 相伴的, 矛盾. 故 $r \neq 0$,

$$d(r) < d(b).$$

又, $a \mid b$, 必有 $c \in D$ 使 $b = ac$, 从而

$$r = a - bq = a - acq = a(1 - cq).$$

用 d 的性质, 即得到

$$d(a) \leqslant d(r) < d(b).$$

在欧氏环中有一种求最大公因子的算法.

例题2 设 D 对映射 d 是个欧氏环. a, $b \in D$ 且 $b \neq 0$. 求 a 和 b 的一个最大公因子.

解 因为 D 是个欧氏环, 必有 q_1, $r_1 \in D$ 使

$$a = bq_1 + r_1, \qquad r_1 = 0 \text{ 或 } d(r_1) < d(b).$$

如果 $r_1 = 0$, 那么 $b \mid a$, b 即为 a, b 的一个最大公因子.

如果 $r_1 \neq 0$, 则必有 $d(r_1) < d(b)$. 又必有 q_2, $r_2 \in D$ 使

$$b = r_1 q_2 + r_2, \qquad r_2 = 0 \text{ 或 } d(r_2) < d(r_1).$$

当 $r_2 = 0$ 时, 算法即停止; 当 $r_2 \neq 0$ 时, $d(r_2) < d(r_1)$ 再做

$$r_1 = r_2 q + r_3, \qquad r_3 = 0 \text{ 或 } d(r_3) < d(r_2).$$

一直做下去.

由于 $d(r_1) > d(r_2) > \cdots$ 且它们都是非负整数，这种做法不会永远做下去，必然有限步停止；即到某一步，出现整除情况. 一般地，可以设

$$\begin{aligned}
a &= bq_1 + r_1, & d(r_1) &< d(b),\\
b &= r_1 q_2 + r_2, & d(r_2) &< d(r_1),\\
r_1 &= r_2 q_3 + r_3, & d(r_3) &< d(r_2),\\
&\cdots\cdots\cdots & &\cdots\cdots\cdots\\
r_{k-2} &= r_{k-1} q_k + r_k, & d(r_k) &< d(r_{k-1}),\\
r_{k-1} &= r_k q_{k+1}.
\end{aligned}$$

可以断言 r_k 就是 a, b 的一个最大公因子.

首先，$r_k | r_{k+1}$，看上列倒数第二个等式，即知 $r_k | r_{k-2}$. 追溯上去，r_k 可整除每一个 r_i. 可是，从第二个等式可以看出 $r_k | b$. 再看第一式，由 $r_k | b$, $r_k | r_1$ 又推知 $r_k | a$，也就是说，r_k 是 b 的因子，也是 a 的因子. 从而，它是 a, b 的一个公因式.

其次，还需证明 a, b 的任意一个公因子 c 可整除 r_k. 这次，我们从上往下看.

c 是 a 和 b 的公因子，第一式表明，必有 $c | r_1$. 于是，在第二式中，由 $c | b$, $c | r_1$ 可推出 $c | r_2$, $\cdots$. 如此下去，c 必然整除 r_k.

所以 r_k 是 a, b 的一个最大公因子.

例题 3　求有理数域上多项式

$$a(x) = x_4 - x_3 - x_2 + 1, \qquad b(x) = x_3 - 1$$

的最大公因子.

解　做除法，得

$$x_4 - x_3 - x_2 + 1 = (x_3 - 1)(x - 1) + (-x_2 + x),$$

$$x_3 - 1 = (-x_2 + x)(-x - 1) + (x - 1),$$

$$-x_2+x=(x-1)(-x).$$

从而知 $x-1$ 是 $a(x)$ 和 $b(x)$ 的一个最大公因子.

例题 4 证明复数环的子环 $G=\{\alpha i+\beta \mid \alpha, \beta \in \mathbf{Z}\}$ 同构于 $\mathbf{Z}[x]/(1+x^2)$.

证明 任取 $f(x) \in \mathbf{Z}[x]$, 用 x^2+1 除之, 得

$$f(x)=q(x)(x^2+1)+(\alpha x+\beta)$$

其中 $\alpha, \beta \in \mathbf{Z}$ 是由 $f(x)$ 唯一确定的.

令

$$\varphi: f(x) \to \alpha i+\beta,$$

容易证明 φ 是 $\mathbf{Z}[x]$ 到 G 的满的环同态.

计算 φ 的核. 由于 $f(x) \in \operatorname{Ker}\varphi$ 的充要条件是 $\alpha=0$, $\beta=0$, 即 $x^2+1 \mid f(x)$, 故

$$\operatorname{Ker}\varphi=(x^2+1),$$

由环同态基本定理知 $\mathbf{Z}[x]/(x^2+1) \cong G$.

习　题

1. 在 $\mathbf{Z}_5[x]$ 中求

$$x^4+4x^3+4x^2+1, \qquad x^3+4$$

的一个最大公因子.

2. 设 D 是个主理想整环, $a, b \in D$ 且 a 和 b 互素. 证明: 如果 $c \in D$, $a \mid (bc)$, 则 $a \mid c$.

3*. 设 R 是个有 1 的交换的主理想环, 且 $f: R \to S$ 是满的环同态映射. 证明: S 必然是主理想环.

4. 求出例题 4 中环 G 的所有单位.

5. 在例题 4 中的环 G 中把元素 $-1+3i$ 分解成素元之积.

6. 设 D 对于映射 d 作成一个欧氏环, $a, b \in D$ 且 $a \mid b$. 证明: 如果 $d(a)=d(b)$, 则 a 和 b 是相伴的.

§3　唯一分解整环上的多项式环

设 F 是个域，那么 F 上的多项式环 $R=F[x]$ 就是个唯一分解整环.

我们又可以讨论整环 $R=F[x]$ 上的关于文字 y 的多项式环 $R[y]$，它是否是唯一分解整环呢？

在第四章 §1，我们看到，环 R 添上一个文字 x 可得 R 上一元多项式环 $R[x]$，在这个环再添加一个文字 y，进一步得环 $R[x][y]=R[x, y]$. 这种添两个文字甚至添多个文字的环在数学分析、高等代数及很多的数学学科中都经常出现. 研究 $R[x]$ 与 $R[x][y]$ 的关系是很有意义的.

这一节，我们将得到一个很一般的结论，当 R 是唯一分解整环时，多项式环 $R[x]$ 也一定是个唯一分解整环，进而 $R[x_1,\cdots,x_n]$ 也是个唯一分解整环. 当 R 为域时，当然更是这样.

设 D 是个唯一分解整环，来研究 $D[x]$.

先把一些已知结论总结一下.

1. $D[x]$ 也是个整环，D 的恒等元 1 就是 $D[x]$ 的恒等元；

2. 对任意 $f(x)$，$g(x)\in D[x]$，因 D 无非零的零因子，故

$$\deg[f(x)g(x)] = \deg f(x) + \deg g(x).$$

3. 若 $f(x)\in D[x]$ 是 $D[x]$ 的单位，由 $f(x)g(x)=1$ 知 $f(x)$ 和 $g(x)$ 均为 0 次，即 D 上的常数多项式，

$$f(x) = u, \qquad g(x) = v, \qquad uv = 1.$$

故 $f(x)$ 是 D 的单位. 而 D 之单位当然是 $D[x]$ 的单位. 这说明，$D[x]$ 和 D 有相同的单位.

4. $f(x)$，$g(x)\in D[x]$ 是相伴的，当且仅当，有 D 的单位 c 使

$$f(x) = cg(x).$$

在初等数学中，已经习惯地把“不含次数更低的非常数因式”的多项式称为不可约多项式. 在 $D[x]$ 中，我们把 $D[x]$ 的素元也称为不可约多项式.

但是，当 D 不为域时，并不是 D 中每个非零元均为 $D[x]$ 的单位. 例如，整数环上多项式 $2(x+1)$ 中，2 和 $x+1$ 都是它的非平凡因子. 所以，对唯一分解整环上多项式分解问题的讨论要比在域上讨论来得麻烦，读者必须注意这个细节.

本节恒设 D 是个唯一分解整环. 于是，D 的任意有限多个不全为 0 的元素必有最大公因子.

定义 1 若 1 是多项式

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, \quad a_i \in D$$

系数 $a_0, a_1, \cdots, a_n$ 的一个最大公因子，则说 $f(x)$ 是 D 上的一个本原多项式.

定理 1(高斯引理) 如果 $f(x)$，$g(x)$ 都是 D 上的本原多项式，那么它们的乘积

$$f(x) = g(x)h(x)$$

也必为 D 上本原多项式.

证明 设

$$g(x) = a_0 + a_1x + \cdots + a_nx^n,$$

$$h(x) = b_0 + b_1x + \cdots + b_mx^m$$

都是 D 上本原多项式. 且

$$f(x) = g(x)h(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n}.$$

如果 $f(x)$ 不是本原多项式，即 $c_0, c_1, \cdots$ 有非单位 d 为其公因子. 将 d 做素因子分解，设 D 的素元 p 是 d 的因子，从而素元 p 是 $c_0, c_1, \cdots, c_{m+n}$ 的一个公因子.

但是，$g(x)$ 和 $h(x)$ 都是本原的，p 不是 $g(x)$ 系数的公因子，p 也不是 $h(x)$ 的系数的公因子. 必有整数 i, j 使 $p \nmid a_i$，

$p \nmid b_j$. 设

$$p \mid a_0, p \mid a_1, \cdots, p \mid a_{r-1}; p \nmid a_r,$$

$$p \mid b_0, p \mid b_1, \cdots, p \mid b_{s-1}; p \nmid b_s.$$

看$f(x)$的系数c_{r+s}，由于

$$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r-1} b_{s+1} + a_r b_s$$

$$+ a_{r+1} b_{s-1} + \cdots + a_{r+s-1} b_1 + a_{r+s} b_0$$

的右端除$a_r b_s$外其余诸项中或者a的脚码小于r或者b的脚码小于s，二因子中总有一个要能被p整除. 又$p \mid c_{r+s}$，故$p \mid (a_r b_s)$.

D是唯一分解整环，p为素元，由§1之定理1知，$p \mid a_r$或$p \mid b_s$，矛盾.

一般来说，如果整环S是整环R的子环，那么，S上的多项式$f(x)$也是R上的多项式. 而且，可能$f(x)$在S上是不可约的，而它作为R上的多项式却是可约的.

例如，有理数环$\mathbf{Q}$上多项式

$$f(x) = x^2 - 2$$

是不可约的，而它作为实数域$\mathbf{R}$上的多项式却有

$$f(x) = (x + \sqrt{2})(x - \sqrt{2}).$$

这样，就为我们的研究提供了一个途径. 讨论S上一个多项式$f(x)$的性质时，先看它在R上的性质，然后再返回到S上来做结论. 当然，我们不是对任意一个包含S的整环R都有兴趣，通常是要求R比S“更好”.

一个域Q称做环R的一个**分式域**，如果Q包含R，且Q恰由形如

$$ab^{-1} = \frac{a}{b}, \quad a, b \in R, b \neq 0$$

的元素组成. 于是若Q是一个整环D的分式域，则$Q[x]$为欧氏环.

命题 1　若 Q 是 D 的分式域. 那么, $Q[x]$ 的非零多项式 $f(x)$ 必可写成如下形式

$$f(x) = \frac{b}{a}f_0(x),$$

其中 $f_0(x)$ 是 $D[x]$ 的本原多项式, $\frac{b}{a} \in Q$. 而且, $f_0(x)$ 在不计相伴的意义下是由 $f(x)$ 来唯一确定的.

证明　设

$$f(x) = \frac{b_0}{a_0} + \frac{b_1}{a_1}x + \cdots + \frac{b_n}{a_n}x^n, \quad \frac{b_i}{a_i} \in Q, \frac{b_n}{a_n} \neq 0.$$

令 $a = a_0a_1\cdots a_n$, 则

$$f(x) = \frac{1}{a}[c_0 + c_1x + \cdots + c_nx^n], \quad c_i \in D, c_n \neq 0.$$

再设 c 是 $c_0, c_1, \cdots, c_n$ 的一个最大公因子, 于是

$$f(x) = \frac{c}{a}[d_0 + d_1x + \cdots + d_nx^n], \quad d_i \in D, d_n \neq 0.$$

此时, 1 必为 $d_0, d_1, \cdots, d_n$ 的一个最大公因子. 若不然, 可设 d 为 $d_0, \cdots, d_n$ 的一个最大公因子, d 不是单位, 于是 cd 就是 $c_0, c_1, \cdots, c_n$ 的一个公因子, 且 cd 不是和 c 相伴的, 与 c 之最大性矛盾.

令

$$f_0(x) = d_0 + d_1x + \cdots + d_nx^n. \qquad (*)$$

则 $f_0(x)$ 是 D 上本原多项式, 且

$$f(x) = \frac{c}{a}f_0(x), \qquad \frac{c}{a} \in Q.$$

进一步, 如果还有 D 上本原多项式 $g_0(x)$,

$$f(x) = \frac{h}{f}g_0(x), \qquad \frac{h}{f} \in Q.$$

那么研究 D 上多项式,

$$l(x) = fcf_0(x) = hag_0(x). \qquad (**)$$

设 q 是 $l(x)$ 的所有系数的一个最大公因子.（**）表明 fc 是 $l(x)$ 所有系数的一个公因子，故有

$$(fc) \mid q, \qquad q = fct, \quad t \in D.$$

又因为 q 是 $fcf_0(x)$ 诸系数的公因子，注意（*），必有

$$fcd_0 = r_0 q, \cdots, fcd_n = r_n q.$$

从而得到

$$d_0 = r_0 t, \cdots, d_n = r_n t.$$

这说明 t 是 $f_0(x)$ 诸系数的一个公因子. 由于 $f_0(x)$ 在 D 上是本原的，故 t 必然是个单位. fc 与 q 是相伴的，fc 是多项式 $l(x)$ 诸系数的一个最大公因子.

同理，ha 也是 $l(x)$ 诸系数的一个最大公因子. 从而 fc 是与 ha 相伴的，有 D 中单位之使得 $ha = \varepsilon fc$. 将其代入（**），用消去律即得

$$fcf_0(x) = \varepsilon fcg_0(x), \qquad f_0(x) = \varepsilon g_0(x);$$

也就是说，如果不考虑相伴的元素的差别时，$f_0(x)$ 是由 $f(x)$ 唯一确定的.

命题 2　设 Q 是 D 的分式域. 那么，D 上的本原多项式 $f(x)$ 在 $D[x]$ 中是可约的，当且仅当，$f(x)$ 在 $Q[x]$ 中是可约的.

证明　若 $f(x)$ 在 $D[x]$ 中是可约的，即 $f(x)$ 在 $D[x]$ 中有非平凡的因子 $h(x)$，即 $h(x) \mid f(x)$ 且 $h(x)$ 不是 $D[x]$ 的单位也不是和 $f(x)$ 相伴的.

假设 $h(x)$ 是 $Q[x]$ 的单位，那么它的次数必为 0，它必为 D 的一个常数多项式 c，$c \neq 0$. 于是导出，在 $D[x]$ 中，$c \mid f(x)$. 而 $f(x)$ 是 D 上本原多项式，故 c 为 $D[x]$ 中的单位，与 $h(x)$ 的假设矛盾.

假设 $h(x)$ 在 $Q[x]$ 中是与 $f(x)$ 相伴的，即有 c，$b \in D$ 使

$$h(x) = \frac{c}{b}f(x), \quad bh(x) = cf(x).$$

若

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$

则 b 应为 ca_0, ca_1, $\cdots$, ca_n 的一个公因子. 但又知 ca_0, $\cdots$, ca_n 的最大公因子是 c, 所以 $b|c$. 有 d 使 $b=cd$,

$$df(x) = h(x), \quad f(x) \mid h(x)$$

导致 $f(x)$ 和 $h(x)$ 在 $D[x]$ 中是相伴的, 矛盾.

这说明 $h(x)$ 既不是 $Q[x]$ 的单位也不是 $f(x)$ 在 $Q[x]$ 中相伴的, $h(x)$ 在 $Q[x]$ 中是 $f(x)$ 的非平凡因子. $f(x)$ 在 $Q[x]$ 中可约.

反过来, 若 $f(x)$ 在 $Q[x]$ 中是可约的. 设

$$f(x) = g(x)h(x), \qquad g(x), h(x) \in Q[x],$$

$g(x)$ 和 $h(x)$ 都是 $f(x)$ 的非平凡因子.

由于域上的非零的常数多项式必为单位, 而 $g(x)$ 和 $h(x)$ 均非零, 所以它们的次数均大于 0. 由命题 1 知, 必有 $D[x]$ 的本原多项式 $g_0(x)$ 和 $h_0(x)$ 使

$$g(x) = \frac{b}{a}g_0(x), \quad h(x) = \frac{d}{c}h_0(x), \quad \frac{b}{a}, \frac{d}{c} \in Q.$$

于是 $f(x) = \frac{b}{a}\frac{d}{c}g_0(x)h_0(x)$.

根据定理 1 可推出 $g_0(x)h_0(x)$ 也是 D 上的本原多项式. 再据命题 1, 必有 D 的单位 ε 使

$$f(x) = \varepsilon g_0(x)h_0(x).$$

这里, $\varepsilon g_0(x)$ 和 $h_0(x)$ 都是 D 上多项式, 均为 $f(x)$ 的因子. $h_0(x)$ 次数与 $h(x)$ 相同, 大于 0, $h_0(x)$ 不是 $D[x]$ 的单位. $\varepsilon g_0(x)$ 也不是环 $D[x]$ 的单位, 从而 $h_0(x)$ 在 $D[x]$ 中不是与 $f(x)$ 相伴的, $h_0(x)$ 为 $f(x)$ 在 $D[x]$ 中的非平凡因子. 即 $f(x)$ 在

$Q[x]$中是可约的.

例题 1　在有理数域上，多项式$f(x)=x^4+3x+1$是否可约？

解　我们只要看$f(x)$是否在$\mathbf{Z}[x]$上可约.

若$f(x)$有一次的非平凡因子

$$f(x)=(ax+b)g(x)$$

比较两端系数，必有$a|1$，$b|1$，故$ax+b$只可能为

$$x+1,\ x-1,\ -x-1,\ -x+1.$$

两个多项式相差-1倍，则是相伴的，故只考虑

$$x+1,\ x-1.$$

若$f(x)=(x+1)g(x)$，则$f(-1)=0$，但$f(-1)=-1$故$(x+1)\nmid f(x)$. 同理$(x-1)\nmid f(x)$. 这说明$f(x)$没有一次的非平凡因子.

若$f(x)$有二次的非平凡因子，其首系数必为±1. 相伴的可以不计，$f(x)$必有首系数为1的二次非平凡因子，故可设有整数a，b，c，d使

$$x^4+3x+1=(x^2+ax+b)(x^2+cx+d).$$

于是下列整数方程组应该有解

$$\begin{cases} a+c=0, \\ b+d+ac=0, \\ bc+ad=3, \\ bd=1. \end{cases}$$

但是，这意味着b，d同时为1或同时为-1，从而$b+d=\pm2$. 同时

$$ac=-a^2=-(b+d),$$

导致$a^2=\pm2$，矛盾.

$f(x)$在$\mathbf{Z}[x]$上不可约，从而在$\mathbf{Q}[x]$上亦不可约.

命题 3　$D[x]$中非常数的本原多项$f(x)$在$D[x]$中有唯一

分解(相伴不计).

证明 首先证明$f(x)$必可写成$D[x]$的不可约多项式之连乘积.

当$f(x)$本身不可约时,目的已经达到.

当$f(x)$可约时,它的非平凡因子不能是常数多项式,故必有

$$g(x),\ h(x)\in D[x],$$

$$f(x)=g(x)h(x),\qquad 1\leqslant \deg g(x)<\deg f(x).$$

再据$f(x)$的本原性知$g(x)$和$h(x)$均为$D[x]$中本原的.

如果$g(x)$或$h(x)$可约,将其分解,有

$$f(x)=k(x)l(x)j(x),$$

其中$k(x)$,$l(x)$和$j(x)$都是非常数的本原多项式.

由于$f(x)$次数有限,最后可得到

$$f(x)=p_1(x)p_2(x)\cdots p_r(x),\tag{$*$}$$

其中$p_i(x)$是$D[x]$上非常数的不可约的本原多项式.

若,又有

$$f(x)=q_1(x)q_2(x)\cdots q_j(x),\tag{$**$}$$

其中$q_j(x)$是不可约的.那么,$q_j(x)$必然是本原的.再由$f(x)$的本原性知$q_j(x)$均不为常数多项式.

根据命题2,$p_i(x)$,$q_j(x)$在$Q[x]$中也是不可约的.但Q是个域,$Q[x]$是个唯一分解整环.在$Q[x]$中看($*$)和($**$),必有$r=s$.调整$q_j(x)$的顺序后,$p_i(x)$和$q_i(x)$在$Q[x]$中是相伴的.设

$$q_i(x)=\frac{b_i}{a_i}p_i(x),\qquad \frac{b_i}{a_i}\in Q.$$

在$D[x]$中就有(据命题1)

$$q_i(x)=\varepsilon_i p_i(x),$$

其中ε_i是D的单位.不计相伴的差别,$p_i(x)$和$q_i(x)$是$f(x)$

的相同的因子.

定理 2 如果 D 是唯一分解整环，则 $D[x]$ 也是唯一分解整环.

证明 任取 $D[x]$ 的一个非 0 非单位的多项式 $f(x)$.

如果 $f(x)$ 是非 0 非单位的常数多项式，即 $f(x)\in D$. 由于 D 是唯一分解整环，$f(x)$ 可以写成 D 的素元的连乘积，也就是 $D[x]$ 的素元之连乘积，且分解唯一.

所以，我们只需考虑 $f(x)$ 不是常数多项式的情形. 可把 $f(x)$ 诸系数之最大公因子提出来，得

$$f(x) = dg(x),$$

其中 $g(x)$ 是 D 上的本原多项式.

如果 d 是 D 的一个单位，则 $f(x)$ 就是 D 上本原多项式，据命题 3，它可唯一地分解.

如果 d 不是 D 的单位，d 在 D 中唯一分解，设

$$d = p_1p_2\cdots p_m,$$

其中 p_i 都是 D 的素元. 同样据命题 3，

$$g(x) = p_1(x)\cdots p_r(x),$$

其中 $p_j(x)$ 都是 $D[x]$ 的不可约多项式. 由于 p_i 也是 $D[x]$ 的素元，

$$f(x) = p_1p_2\cdots p_mp_1(x)p_2(x)\cdots p_r(x).$$

已写成 $D[x]$ 之素元乘积形式.

设 $f(x)$ 还有一素元积形式. 我们总可以调整顺序，让那些属于 D 的在前，不属于 D 的列后，即不妨设为

$$f(x) = q_1\cdots q_nq_1(x)\cdots q_s(x),$$

其中 $q_i\in D$, $q_j(x)\notin D$.

这里 q_i 是 $D[x]$ 的素元，当然就是 D 的素元. 而 $q_j(x)$ 必然是非常数的本原多项式，否则其系数的最大公因子 d 不是单位，从而是 $q_j(x)$ 的一个非平凡因子.

于是，先由定理 1 知

$$p_1(x)\cdots p_r(x) \text{ 和 } q_1(x)\cdots q_s(x)$$

均为本原多项式，再由

$$p_1(x)\cdots p_r(x) = \frac{q_1\cdots q_n}{p_1\cdots p_m} q_1(x)\cdots q_s(x)$$

和命题 1 知有 D 的单位 ε 使

$$p_1(x)\cdots p_r(x) = \varepsilon q_1(x)\cdots q_s(x), \qquad (*)'$$

$$\varepsilon p_1 p_2\cdots p_m = q_1 q_2\cdots q_n. \qquad (**)'$$

把 D 元唯一分解性用到$(**)'$上，得 $m=n$，调整顺序后 p_i 和 q_i 是相伴的.

把命题 3 用到$(*)'$上，得 $r=s$，且调整顺序可使 $p_j(x)$ 与 $q_j(x)$ 相伴.

这就是最终证明了唯一分解性.

习　题

1. 证明，多项式 x^4+2x+2 在有理数域 $\mathbf{Q}$ 上是不可约的.

2. 设 p 是个素数，$f(x)$，$g(x)$，$h(x)\in\mathbf{Z}[x]$，且 $pf(x)=g(x)h(x)$，p 不整除 $g(x)$ 的首项系数，证明，$h(x)$ 的每个系数均能被 p 整除.

3. 问，在 $\mathbf{Z}_5[x]$ 中多项式 x^3+x^2+1 是不是素元.

第六章　域

域，这个特殊的结合环，其每个非零元均有乘法逆，导致它的结构有极好的特殊性，如无零因子、无非平凡理想等. 用域的理论处理各种域与其子域之间的关系，它起源于 Abel 和 Galois 研究代数方程根式解问题.

域论是代数学中重要基础之一，是现代代数学许多分支（如代数几何、代数数论）的基础.

§1　域及其子域

第四章 §5 给出了域的定义，现在略深入地研究一下域的性质并介绍几种典型的域.

命题 1　只含有限个元素的整环必为域.

证明　设 R 是有限整环，1 为其恒等元. 任取 $a\in R$, $a\neq 0$，看元素

$$a,\ a^2,\ \cdots,\ a^n,\ \cdots,$$

由于 R 的有限性，上述元素必有重复，不妨设有正整数 k, l 使

$$a^k = a^l,\quad k < l,$$

但 $a^l = a^k\cdot a^{l-k}$，即

$$a^k(1 - a^{l-k}) = 0.$$

但 $a\neq 0$，从而不为零因子，推出

$$1 - a^{l-k} = 0,$$

也就是

$$a^{l-k-1}\cdot a = 1,$$

a 有逆元.

命题 2 设 F 是个域. 如果有 $a \in F$, $a \neq 0$ 及正整数 n 使 $na = 0$, 那么, 必有唯一确定的素数 p, 对任意 $x \in F$ 都有 $px = 0$.

证明 如果 n 不是素数, 那么必有素数 p_1, 使 $n = p_1 n_1$. 令 e 代表 F 的恒等元, 则得

$$na = (p_1 n_1) a = (p_1 e)(n_1 a),$$

由于域无零因子, 故

$$p_1 e = 0 \quad 或 \quad n_1 a = 0.$$

若 $p_1 e_1 = 0$, 那么, 对任意 $x \in F$, 均有

$$p_1 a = (p_1 e) a = 0.$$

若 $n_1 a = 0$, 仿上继续下去, 最终得整数 p, 使对任意 $x \in F$, $px = 0$.

如果有素数 p, q 均有上述性质, 且 $p \neq q$, 设有整数 r, s 使

$$pr + qs = 1,$$

于是导致

$$x = (pr + qs)x + r(px) + s(qx) = 0,$$

矛盾.

定义 1 若素数 p 对域 F 的每个元 x 均有 $px = 0$, 则说 F 的特征数为 p, 其余情形说 F 之特征数为 0.

定义 2 域 F 的子环 S 本身是个域, 则称 S 为 F 的一个子域, F 是 S 的一个扩张域.

命题 3 若域 F 的特征数为 p, 1 是 F 的恒等元, 则

$$S = \{0, 1, \cdots, p-1\}$$

是 F 的一个子域, 且它含在 F 的每个子域中.

证明 任取 m, $n \in S$, 必有 q, $r \in \mathbf{Z}$ 使

$$m + n = pq + r, \quad 0 < r < p$$

而 $pq = 0$, 这说明 $m + n = r \in S$, 同理 $mn \in S$.

进一步，若 $m\in S$，$m\neq 0$，由于 p 是素数，必有 $r, s\in \mathbf{Z}$，使

$$mr+ps=1$$

以及

$$r=pk+t,\quad 0\leqslant t<p.$$

于是

$$mt=mr+ps=1,$$

这说明 t 是 s 的逆.

命题 4　若域 F 的特征数为素数 p，那么，对任意 $a, b\in F$ 均有

$$(a+b)^p=a^p+b^p.$$

证明　用二项式定理，得

$$(a+b)^p=a^p+pa^{p-1}b+\cdots+pab^{p-1}+b^p,$$

F 之特征数为 p，右端除首项与末项外均为 0，故

$$(a+b)^p=a^p+b^p.$$

例题　已知域 F 只含四个元素 0，1，a，b，且其特征数为 2，试列出其加法表和乘法表.

解　对任意 $x\in F$，$2x=0$，即 $x=-x$. 再根据消去律，必有 $a+b=1$，

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

对于乘法，由于 $\{1, a, b\}$ 是个 Abel 乘群，只需考虑 a^2. 若 $a^2=1$，由命题 4 必有

$$0=a^2+1=(a+1)^2=b^2.$$

故知 $a^2=b$，$b^2=a$. 乘法表为

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

习　题

1. 证明，所有的三元域都是同构的环.

§2　域的单纯扩张

定义1　设E是域F的一个扩张域，S是E的一个子集，E中由$F\cup S$生成的子域，记为$F(S)$，称为是F上添加S得到的子域. 当$S=\{a_1, a_2, \cdots, a_n\}$时，记

$$F(S) = F(a_1, \cdots, a_n),$$

当$E=F(a)$时，说E是F的一个**单纯扩张域**，或E是F的**单纯扩张**.

例如，复数域是实数域$\mathbf{R}$添加$\mathrm{i}=\sqrt{-1}$而成的，故

$$\mathbf{C} = \mathbf{R}(\mathrm{i}).$$

现在看$\mathbf{R}$的单纯扩张$\mathbf{R}(2+\sqrt{-3})$.

由于

$$2+\sqrt{-3} = 2+\mathrm{i}\sqrt{-3} \in \mathbf{R}(\mathrm{i}),$$

故$\mathbf{R}(2+\sqrt{-3})\leqslant\mathbf{R}(\mathrm{i})$. 另一方面，由

$$\mathrm{i} = [(2+\mathrm{i}\sqrt{3})-2]\frac{1}{\sqrt{3}} \in \mathbf{R}(2+\sqrt{-3}),$$

知$\mathbf{R}(\mathrm{i})\leqslant\mathbf{R}(2+\sqrt{-3})$. 故$\mathbf{R}(\mathrm{i})=\mathbf{R}(2+\sqrt{-3})$.

这说明，同一个域上不同添加可能得相同的扩张域.

下面讨论单纯扩张的结构.

对于域 F 上的多项式环 $F[x]$，可以像数域上一元多项式一样研究其所有分式构成的环，

$$F\{x\} = \{f(x)/g(x) \mid f(x),\ g(x) \in F[x],\ g(x) \neq 0\},$$

容易证明 $F\{x\}$ 是个域，称为 $F[x]$ 的分式域.

命题 1　设 E 是 F 的单纯扩张，$E=F(a)$. 那么，或者 E 同构于 $F[x]$ 的分式域 $F\{x\}$，或者有 F 上的不可约多项式 $p(x)$ 使

$$F(a) \cong F[x]/(p(x)).$$

证明　对于 E 中有 $F\cup\{a\}$ 生成的子环 $F[a]$，建立映射

$$\varphi: F[x] \to F[a],$$

$$\varphi: f(x) \to f(a),$$

这是多项式环 $F[x]$ 到环 $F[a]$ 的一个环同态. 由环同态基本定理，知

$$F[a] \cong F[x]/\mathrm{Ker}\varphi,$$

其中 $\mathrm{Ker}\varphi$ 是 $F[x]$ 的一个理想. 但 $F[x]$ 是主理想环，必有不可约多项式 $p(x)$ 使 $\mathrm{Ker}\varphi=(p(x))$，或者 $\mathrm{Ker}\varphi=\{0\}$.

若 $\mathrm{Ker}\varphi=(p(x))$，$p(x)\in F[x]$ 不可约，那么商环 $F[x]/(p(x))$ 为域，即 $F[a]$ 同构于域 $F[x]/(p(x))$. 由于 $F[x]\subseteq F[a]$，$F(a)$ 是 E 中由 $F\cup\{a\}$ 生成的最小子域，现又已知 $F[a]$ 为域，故 $F(a)=F[a]$，即 $F(a)$ 同构于 $F[x]/(p(x))$.

再注意到 $\mathrm{Ker}\varphi=(p(x))$，即 $p(a)=0$，这说明 a 满足 $F[x]$ 的不可约多项式 $p(x)$.

若 $\mathrm{Ker}\varphi=\{0\}$，则 $F[a]\cong F[x]$，进而 $F[x]$ 的分式域

$$F\{x\} = \{f(x)/g(x) \mid f,\ g \in F[x],\ (f,\ g) = 1\}$$

同构于

$$F(a) = \{f(a)/g(a) \mid f,\ g \in F[x],\ (f,\ g) = 1\}.$$

定义 2 设 E 是 F 的扩张. 对 E 的任意元 a, 如果有 $F[x]$ 的不可约多项式 $p(x)$ 使 $p(a)=0$, 则说 a 是 F 上的一个**代数元**, 如果 a 不满足 $F[x]$ 上的任何非零多项式, 则说 a 是 F 上的一个**超越元**. 如果 F 的扩张域 E 的每个元都是 F 上的代数元, 则说 E 是 F 的一个**代数扩张**.

例如, 在实数域 $\mathbf{R}$ 中, $\sqrt{2}$是有理数域 $\mathbf{Q}$ 的一个代数元, 因为它满足 x^2-2, 而圆周率 π、自然对数底 e 和 $2^{\sqrt{2}}$均已被证明是 $\mathbf{Q}$ 上的超越元. 又如, 复数域 $\mathbf{C}$ 是实数域 $\mathbf{R}$ 的代数扩张.

设 E 是 F 的扩张域. 我们视 E 为加群, 视 E 中的乘法为 $F\times E\to E$ 的纯量乘, 则显然有

1. 对任意 $a\in F$ 及 $u, v\in E$, $a(u+v)=au+av$;
2. 对任意 $a, b\in F$ 及 $u\in E$, $(a+b)u=au+bu$;
3. 对任意 $a, b\in F$ 及 $u\in E$, $(ab)u=a(bu)$;
4. 对任意 $u\in E$, $1u=u$.

这说明 E 是 F 上的一个线性空间.

对于一般域上的线性空间, 可仿照数域上的线性空间理论, 讨论线性相关性、基底和维数等, 得到相应的结论.

定义 3 如果扩张域 E 是 F 上的有限维线性空间, 则说 E 是 F 的一个**有限扩张**, 其维数记为$[E:F]$.

例如, 复数域 $\mathbf{C}$ 是实数域 $\mathbf{R}$ 上的二维空间, $\{1, \mathrm{i}\}$构成一个基底, 而实数域 $\mathbf{R}$ 在有理数域 $\mathbf{Q}$ 上是无穷维的, $1, \pi, \pi^2, \cdots$是一组线性无关的向量.

命题 2 设 a 是域 F 上的一个代数元, a 满足 F 上不可约多项式

$$f(x)=\alpha_0+\alpha_1x+\cdots+\alpha_nx^n,\quad \alpha_n\neq 0,$$

则$[F(a):F]=n$.

证明 由命题 1 知, 此时 $F(a)=F[a]$, 但对 F 上的任意次多项式 $f(x)$, 必有

$$f(x) = q(x)p(x) + r(x),$$
$$r(x) = 0 \quad 或 \quad r(x) 次数小于 n,$$

于是

$$f(a) = q(a)p(a) + r(a) = r(a),$$

这说明

$$F(a) = \{r(a) \mid r(x) \in F(x), 次 r(x) < n\}.$$

也就是说 $F(a)$ 的每个元素均可由 $1, a, \cdots, a^{n-1}$ 线性表示出来，而且由于 $p(x)$ 不可约，这组向量 $1, a, \cdots, a^{n-1}$ 必然是不可约的. 这样就找到了一组基底，故 $[F(a):F] = n$.

命题 3　若域 E 是域 F 的 n 维扩张，那么 E 的每个元素都是 F 上的代数元.

事实上，任取 $a \in E$，元素

$$1, a, a^2, \cdots, a^n$$

在 F 上必是线性相关的，即必有不全为 0 的 $\alpha_0, \alpha_1, \cdots, \alpha_n \in F$，使

$$\alpha_0 + \alpha_1 a + \cdots + \alpha_n a^n = 0,$$

也就是说 a 满足 F 上非零多项式，进一步必满足一不可约多项式，a 为 F 上代数元.

命题 4　E 是 F 的 n 维扩张，D 是 E 的 m 维扩张，则 D 为 F 的 mn 维扩张.

事实上，若 $a_1, \cdots, a_n$ 为 E 在 F 上的一个基底，$b_1, \cdots, b_m$ 为 D 在 E 上的一个基，那么 $a_i b_j \in D$ $(i=1, 2, \cdots, n; j=1, 2, \cdots, m)$ 恰好为 D 在 F 上的一个基. 从而

$$[D: F] = [D: E][E: F].$$

定理　设 E 是 F 的扩张域，$a, b \in E$ 是 F 上的代数元，那么 $a+b$，$a-b$ 和 ab 都是 F 上代数元，当 $b \neq 0$ 时，ab^{-1} 亦为代数元.

证明　因为 a 是 F 上代数元，故 $F[a]$ 是 F 的有限扩张.

而 b 是 F 上代数元，当然 b 是 $F[a]$ 上的代数元，从而 $E=F[a][b]$ 是 $F[a]$ 上有限扩张，进而知 E 为 F 的有限扩张，它的每个元都是 F 上代数元，这包括 $a+b$，$a-b$，ab 以及 $b\neq 0$ 时的 ab^{-1}.

例题 证明 $\mathbf{Q}(\sqrt{2},\sqrt{3})$ 为 $\mathbf{Q}$ 的单纯扩张，且

$$[\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}]=4.$$

解 一方面，显然有

$$\mathbf{Q}(\sqrt{2}+\sqrt{3})\leqslant\mathbf{Q}(\sqrt{2},\sqrt{3}),$$

另一方面

$$\sqrt{3}-\sqrt{2}=(\sqrt{3}+\sqrt{2})^{-1}\in\mathbf{Q}(\sqrt{2}+\sqrt{3}),$$

从而

$$\sqrt{3}=\frac{1}{2}(\sqrt{3}-\sqrt{2})+\frac{1}{2}(\sqrt{3}+\sqrt{2})\in\mathbf{Q}(\sqrt{2}+\sqrt{3}),$$

同理 $\sqrt{2}\in\mathbf{Q}(\sqrt{2}+\sqrt{3})$，故

$$\mathbf{Q}(\sqrt{2}+\sqrt{3})=\mathbf{Q}(\sqrt{2},\sqrt{3}).$$

可以断言，$\sqrt{3}\notin\mathbf{Q}(\sqrt{2})$. 否则，必有 $r,s\in\mathbf{Q}$ 使得

$$\sqrt{3}=r\sqrt{2}+s,$$
$$3-2r^2-s^2=2rs\sqrt{2}$$

必有 $rs=0$. 但 $r=0$，则 $s\notin\mathbf{Q}$；$s=0$ 则 $r\notin\mathbf{Q}$. 矛盾.

$\sqrt{3}$ 在 $\mathbf{Q}$ 上满足 x^2-3，它在 $\mathbf{Q}(\sqrt{2})$ 必满足一个能整除 x^2-3 的不可约多项式 $p(x)$，若 $p(x)$ 为一次的，则 $\sqrt{3}\in\mathbf{Q}(\sqrt{2})$. 不可能. 故 $p(x)$ 为二次多项式. 于是

$$\begin{aligned}&[\mathbf{Q}(\sqrt{2}+\sqrt{3}):\mathbf{Q}]\\&=[\mathbf{Q}(\sqrt{2},\sqrt{3}):\mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}):\mathbf{Q}]\\&=2\times 2=4.\end{aligned}$$

习　题

1. 设域含 m 个元素，那么，对任意元素 a 都有 $a^m=a$.

2. 设域 F 的特征数为 p，那么

$$S=\{a\in F\mid \text{有自然数 } n \text{ 使 } a^{p^n}=a\}$$

是 F 的一个子域.

第七章　模

在线性代数学中，数域上的线性空间是最基本又最重要的概念. 它有由一个域作用在一个加法群上而产生的代数结构，概括了自然科学和社会科学的大量现象. 随着科学的发展，迫使人们考虑把线性空间中的数域推广到结合环的情形，这就形成了一门很有用的学科——模的理论.

§1　模的定义

定义1　设 R 是个有1环，M 是个交换群. 如果有 $R\times M$ 到 M 的映射

$$(r,\ m)\to rm,\quad r\in R,\ m\in M \tag{1}$$

满足：对一切 $r,\ s\in R,\ m,\ n\in M$ 均有

$$\begin{aligned} r(m+n) &= rm+rn, \\ (r+s)m &= rm+sm, \\ (rs)m &= r(sm), \\ 1m &= m, \end{aligned}$$

则说 M 是个(左) R 模，称映射(1)为 R 到 M 的纯量乘.

对称地可定义右 R 模.

例1　若 V 是数域 F 上的线性空间，则 V 是个 F 模.

例2　设 S 为有1环 R 的有1子环，用 R 的乘法定义 S 到 R 的纯量乘，则 R 为 S 模. 特别，R 本身是 R 模.

例3　设 A 为环 R 的一个加法子群，若对任意 $a\in A,\ r\in R$ 恒有 $ra\in A$，则称 A 为 R 的一个左理想(对称地可定义环的右

理想). 当 R 为有 1 环时, A 为 R 模.

下面讨论模的简单性质. 本章中如不声明, R 表一有 1 环, M 表一加法群, 0 是 R 的零元, θ 是 M 的零元, R 的单位元就记为 1_R 或 1.

命题 1　设 M 是个 R 模, 则对任意 $r\in R$ 及 $x\in M$ 有

$$r\theta = \theta, \qquad 0x = \theta.$$

证明　由

$$r\theta = r(\theta + \theta) = r\theta + r\theta$$

知 $r\theta=\theta$. 同理, 由

$$0x = (0+0)x = 0x + 0x$$

知 $0x=\theta$.

命题 2　设 M 是个 R 模, 则对任意 $r\in R$, $x\in M$ 有

$$-(rx) = (-r)x = r(-x).$$

证明　此由

$$(-r)x + rx = (-r+r)x = 0x = \theta,$$
$$r(-x) + rx = r(-x+x) = r\theta = \theta.$$

即知.

推论　若 M 是 R 模, 则对任意 $x, y\in M$ 及 $r, s\in R$ 有

$$r(x-y) = rx - ry,$$
$$(r-s)x = rx - sx.$$

证明　仅证第一式.

$$r(x-y) = rx + r(-y) = rx - ry.$$

与群论、环论、线性空间理论一样, 可以讨论模的子系统, 由于已有多次训练, 这里的叙述可以简略些了.

定义 2　设 M 是 R 模. 如果 M 的子群 N 对已有的 R 到 M 的纯量乘法也是个 R 模, 则说 N 是 M 的 R **子模**, 简称**子模**.

命题 3　设 M 是 R 模. 那么 M 的非空子集 N 为 R 子模的充分必要条件是:

1. 对任意 $x, y \in N$, 有 $x+y \in N$;

2. 对任意 $r \in R$, $x \in N$, 有 $rx \in N$.

命题 4 设 M 是 R 模, M_i, $i \in I$ 都是 M 的 R 子模, 那么交集 $\bigcap_{i \in I} M_i$ 也是 M 的 R 子模.

定义 3 设 N 是 R 模 M 的子模, 规定 R 对商群 M/N,

$$(r, m+N) \to rm+N, \quad m+N \in M/N, r \in R,$$

则 M/N 成为 R 模, 称为 M 对 N 的 **R 商模**.

这里只需强调, N 为 R 子模保证了上述纯量乘定义的合理性.

习　题

1. 对任意交换群, 规定 $\mathbf{Z} \times G \to G$ 的映射

$$(n, g) \to ng, \quad n \in \mathbf{Z}, g \in G,$$

则 G 是 $\mathbf{Z}$ 模.

2. 设 G 是个交换群, E 是 G 的所有自同态构成的环(见第四章 §1), 规定, 对任意 $\sigma \in E$, $x \in G$,

$$(\sigma, x) \to \sigma(x),$$

则 G 是 E 模.

3. 设 M 是 R 模, I 是 R 的真双边理想, 规定, 对任意

$$(r+I, x) \to rx, \quad r \in R, x \in M,$$

则 M 是 R/I 模.

§2　正合列

定义 1 设 M、N 都是 R 模,

$$\sigma: M \to N$$

是映射, 且满足下列两条要求, 则说 σ 是 **R 模同态**:

1. 对任意 $x, y \in M$ 都有

$$\sigma(x+y)=\sigma(x)+\sigma(y);$$

2. 对任意 $r \in R$, $x \in M$ 都有

$$\sigma(rx)=r\sigma(x).$$

这意味着，σ 首先是 M 到 N 的群同态. 因此，σ 作为两群之间的同态映射，就可以讨论 σ 的核、象等等，可以推出一系列简单的结论.

定义 2　设 $M_i(i \in \mathbf{Z})$ 是 R 模，

$$f_i: M_{i-1} \to M_i, \quad i \in \mathbf{Z}$$

是 R 模同态. 如果对每个 $i \in \mathbf{Z}$ 都有

$$\mathrm{Img}(f_i)=\mathrm{Ker}(f_{i+1}),$$

则说

$$\cdots \xrightarrow{f_{i-1}} M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

是个**正合列**.

用 0 代表只含一个零元的 R 模，称为**零模**.

命题 1　若 $f: M \to N$ 是 R 模单同态，则

$$0 \longrightarrow M \xrightarrow{f} N$$

是正合的，若 f 是 R 模的满同态，则

$$M \xrightarrow{f} N \longrightarrow 0$$

是正合的.

命题 2　设 N 是 M 的 R 子模，

$$j: N \to M,$$
$$j: x \to x$$

是嵌入映射，而

$$\gamma: M \to M/N,$$
$$\gamma: c \to x+N$$

是自然映射，那么

$$0 \longrightarrow N \xrightarrow{j} M \xrightarrow{\gamma} M/N \longrightarrow 0$$

是正合的.

证明 两端的正合性据命题 2 可得，而

$$\mathrm{Img}(j) = \mathrm{Ker}(\gamma)$$

恰说明中项正合.

定理 1 设交换图

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \xrightarrow{f} & M & \xrightarrow{g} & P & \longrightarrow & 0 \\ & & \downarrow{\sigma} & & \downarrow{\tau} & & \downarrow{\rho} & & \\ 0 & \longrightarrow & A & \xrightarrow{h} & B & \xrightarrow{i} & C & \longrightarrow & 0 \end{array}$$

中两横行是正合的，而 σ，τ，ρ 都是单射. 那么 τ 为同构映射的充分必要条件是 σ，ρ 为同构映射.

证明 设 τ 为同构映射. 任取 $a \in A$，$h(a) \in B$，由于 τ 是个满射，必有 $m \in M$ 使 $\tau(m) = h(a)$. 注意正合性，应有

$$h(a) \in \mathrm{Img}(h) = \mathrm{Ker}(i),$$

从而 $ih(a) = 0$. 再由图的交换性知 $i\tau = \rho g$，故

$$\rho g(m) = i\tau(m) = ih(a) = \theta.$$

但 ρ 是单射，知 $g(m) = \theta$，$m \in \mathrm{Ker}(g) = \mathrm{Img}(f)$，即有 $n \in N$ 使 $m = f(n)$，从而有

$$h\sigma(n) = \tau f(n) = \tau(m) = h(a).$$

由 h 是单射，知 $a = \sigma(n)$. 由 $a \in A$ 的任意性知 σ 是满射. 已知 σ 是单射，故 σ 是同构. 以下证明 ρ 是满射，即可知 ρ 是同构. 设 $c \in C$，由 i 是满射知有 $b \in B$ 使 $c = i(b)$. 由 τ 是满射，有 $m \in M$ 使 $\tau(m) = b$. 于是有

$$\rho g(m) = i\tau(m) = i(b) = c,$$

知 ρ 是满射.

反之，设 σ 和 ρ 是同构，$b\in B$. 由 $i(b)\in C$，ρ 是满射知有 $P\in P$ 使 $\rho(p)=i(b)$. 由 g 是满射有 $n\in M$ 使 $g(m0=p$，从而有

$$i(b)=\rho(p)=\rho g(m)=i\tau(m),$$

故有

$$i(b-\tau(m))=\theta,$$
$$b-\tau(m)\in \mathrm{Ker}(i)=\mathrm{Img}(h),$$

于是有 $a\in A$ 使

$$b-\tau(m)=h(a).$$

由 σ 是同构有 $b\in N$ 使 $\sigma(n)=a$，故有

$$b=\tau(m)+h\sigma(n)=\tau(m)+\tau f(n)=\tau(m+f(n)),$$

知 τ 是满射从而为同构.

这种定理的证明分了很多步骤，用到的条件也比较多. 如果不利用图表只靠想象力，证起来是很困难的.

像刚刚做过的那样，充分利用图表，随时注意每个元的归属，再注意所属模的相关映射的正合性、满性、单性，一步一步或进或退，就自然明了些. 这种证明方法常称为图表追赶法.

习　　题

1. 设 M 是 R 模，证明下列说法等价：

(a) M 没有真子模；

(b) 任意非零 R 同态映射 f: $M\to N$ 都是单射；

(c) 任意非零 R 同态映射 g: $P\to M$ 都是满射.

2. 设 f: $M\to N$, g: $N\to P$ 都是 R 模同态映射. 证明，若 f, g 都是单射，则 gf 亦为单射；若 f, g 为满射，则 gf 亦为满射；若 gf 是单射，则 f 是单射；若 gf 是满射，则 g 是满射.

§3 模的张量积

线性空间的张量积是多重线性代数学中基础性概念之一，是几何学、力学中常用的数学工具. 本节讨论模的张量积理论是线性代数理论的推广，是进一步学习群论、交换代数学、Lie 代数和 Hopf 代数等学科的理论基础. 同时，它有来自拓扑学、量子场论等的学科背景.

定义 1 设 R 是个有 1 交换环，X 是任意一个非空集合. 看形式符号的集合

$$T = \{y = r_1x_1 + \cdots + r_nx_n\},$$

其中 $r_i \in R$, $x_i \in X$, $i = 1, 2, \cdots, n$, 诸 x_i 两两不同. 称 r_i 为 y 的 x_i 项系数. 规定，若 y 的 x_j 项系数 $r_j = 0$，则此项可写可不写（这是一种等价关系）. T 中两元相等，如果其每项系数都对应相同.

进一步，对 T 中任意两个形式符号 y, z，选取统一表达式时，如

$$y = t_1x_1 + \cdots + t_mx_m,$$

$$z = s_1x_1 + \cdots + s_mx_m,$$

规定加法运算

$$y + z = (t_1 + s_1)x_1 + \cdots + (t_m + s_m)x_m,$$

及纯乘运算

$$ry = (rt_1)x_1 + \cdots + (rt_m)x_m, \quad r \in R.$$

称 T 对上述运算构成的 R 模为 X 上的 R **自由模**.

定义 2 设 R 是个交换环，M 和 N 都是 R 模，F 是笛卡尔积 $M \times N$ 上的 R 自由模，

$$F = \left\{ \sum_{i,j} r_{ij}(x_i, y_j) \,\middle|\, r_{ij} \in R, x_i \in M, y_j \in N \right\}.$$

再把 F 中形如

$$(x_1 + x_2, y) - (x_1, y) - (x_2, y),$$

$$(x, y_1 + y_2) - (x, y_1) - (x, y_2),$$

$$(rx, y) - (x, ry)$$

的元分别称为 F 的第一类、第二类和第三类元，其中 $x, x_1, x_2 \in M$, $y, y_1, y_2 \in N$, $r \in R$. F 的由所有的三种元生成的子模记为 G.

称商群 F/G 为 M, N 的张量积，记为 $M \otimes_R N$, 并记

$$\sum l_{ij}(x_i, y_j) + G = \sum l_{ij}(x_i \otimes y_j).$$

例 1 对于整数环 $\mathbf{Z}$, 把 $\mathbf{Z}/(2) = \{[0],[1]\}$ 和 $\mathbf{Z}/(3) = \{[0],[1],[2]\}$ 看成 $\mathbf{Z}$ 模. 那么，集合 $\mathbf{Z}/(2) \times \mathbf{Z}/(3)$ 上的自由 $\mathbf{Z}$ 模的一般元素为

$$k([0],[1]) + l([0],[2]) + p([1],[0]) + q([1],[1]) + m([1],[2]),$$

其中 $k, l, p, q, m \in \mathbf{Z}$.

F 中，元

$$\begin{aligned} &([0],[2]) + ([0],[1]) \\ &= ([0],[2]) - 2([0],[1]) \\ &= ([0],[2]) - ([0],[1]) - ([0],[1]) \end{aligned}$$

为第二类元，而元

$$([0],[1]) - ([1],[2]) = (2[1],[1]) - ([1],2[1])$$

为第三类元.

张量积 $\mathbf{Z}/(2) \otimes_{\mathbf{Z}} \mathbf{Z}/(3)$ 的元素必形如

$$\sum t_{ij}(x_i \otimes y_j) = \sum t_{ij}(x_i, y_j) + G.$$

看其中任意一项

$$x \otimes y = (x, y) + G, \quad x \in \mathbf{Z}/(2), y \in \mathbf{Z}/(3).$$

看 $([1],[y])$, 由于在 $\mathbf{Z}/(2)$ 中 $-[1] = [-1] = [1]$, 从

而在 F 中有

$$([1],[y]) = ([1],[y]) - ([1],[y]) - ([1][y]),$$

这说明在$([1],[y]) \in G$，对任何 $y \in \mathbf{Z}$ 都成立，也就是说

$$[1] \otimes [y] = 0,$$

其中右端的 0 乃是张量积 $\mathbf{Z}/(2) \otimes \mathbf{Z}/(3)$ 中的零元.

为计算方便，我们先推演一些简单公式. 本节 R 均指有 1 交换环；M，N 为 R 模；张量积 $M \otimes_R N$ 中的零元也简记为 0.

命题 1 对任意 x_1，$x_2 \in M$；y_1，$y_2 \in N$；$r \in R$ 都有

$$(x_1 + x_2) \otimes y = x_1 \otimes y_1 + x_2 \otimes y_1,$$

$$x_1 \otimes (y_1 \otimes y_2) = x_1 \otimes y_1 + x_1 \otimes y_2,$$

$$(rx) \otimes y = x \otimes ry.$$

证明 由于

$$\begin{aligned} &(x_1 + x_2) \otimes y_1 - x_1 \otimes y_1 - x_2 \otimes y_1 \\ =& [(x_1 + x_2, y_1) - (x_1, y_1) - (x_2, y_1)] + G \\ =& G \\ =& 0, \end{aligned}$$

知第一式成立，同法可证其余两式.

命题 2 对任意 $x \in M$，$y \in N$，有

$$x \otimes 0 = 0, \qquad 0 \otimes y = 0.$$

证明 由于

$$(0, y) = (0, y) + (x, y) - (0 + x, y) \in G,$$

故 $0 \otimes y = 0$.

从例 1 中我们已经看到，在张量积中. 可能 $x \neq 0$，$y \neq 0$ 但 $x \otimes y = 0$. 实际上，$\mathbf{Z}/(2) \otimes_{\mathbf{Z}} \mathbf{Z}/(3)$ 只含一个零元，因为$[1] \otimes [y] = 0$，$[0] \otimes [y] = 0$，对任意 $y \in \mathbf{Z}$ 都成立.

模的张量积有所谓的泛性，它刻画了张量积的本质特性，运用起来也非常方便.

定义 3　设 R 是个交换环，M 和 N 是 R 模，T 是个交换群. 由笛卡尔积 $M\times N$ 到 T 的映射称为**平衡映射**，如果，对任意 x，x_1，$x_2\in M$，y，y_1，$y_2\in N$ 及 $r\in R$ 恒有

$$f(x_1+x_2,\ y)=f(x_1,\ y)+f(x_2,\ y),$$

$$f(x,\ y_1+y_2)=f(x,\ y_1)+f(x,\ y_2),$$

$$f(x,\ ry)=f(rx,\ y).$$

例如，规定

$$f:\ M\times N\to M\otimes_R N,$$

$$f:\ (x,\ y)\to x\otimes y,$$

则 f 是 $M\times N$ 到 $M\otimes_R N$ 的一个平衡映射.

定理 1　设 R 是交换环，M 和 N 是 R 模，φ 是 $M\times N$ 到交换群 P 的一个平衡映射，且

$$f:\ M\times N\to M\otimes_R N,$$

$$f:\ (x,\ y)\to x\otimes y.$$

那么，必有 $M\otimes_R N$ 到 P 的唯一一个群同态映射 f^*，使图

$$\begin{array}{ccc} M\times N & \xrightarrow{\ f\ } & M\otimes_R N \\ & \searrow^{\varphi} & \downarrow{f^*} \\ & & P \end{array}$$

交换.

证明　规定 $M\times N$ 上的 R 自由模 F 到 P 的一个映射

$$h:\ F\to P,$$

$$h:\ \sum r_i(x_i,\ y_i)\to\sum_i r_i\varphi(x_i,\ y_i),\quad r_i\in R.$$

易知 h 是个群同态. 任取 F 中的一个第一类元素

$$a=(x_1+x_2,\ y)-(x_1,\ y)-(x_2,\ y),$$

则

$$h(a) = \varphi(x_1 + x_2, y) - \varphi(x_1, y) - \varphi(x_2, y),$$

而 φ 是平衡映射，故 $h(a)=0$，即 $a \in \mathrm{Ker}(h)$. 进一步知 F 中三型元生成的子群 G 含于 h 的核.

规定 $M \otimes_R N = F/G$ 到 P 的映射

$$f^* : \sum r_{ij}(x_i \otimes y_j) \to \sum r_{ij}\varphi(x_i, y_j).$$

先来说明定义的合理性. 若

$$\sum l_{ij}(x_i \otimes y_j) = \sum k_{st}(u_s \otimes v_t),$$

其中 l_{ij}, $k_{st} \in R$; x_i, $u_s \in M$; y_j, $v_t \in N$, 则说明

$$\sum l_{ij}(x_i, y_j) - \sum k_{st}(u_s, v_t) \in G \subseteq \mathrm{Ker}(h),$$

从而

$$h\left[\sum l_{ij}(x_i, y_j) - \sum k_{st}(u_s, v_t)\right] = 0,$$

也就是

$$\sum l_{ij}\varphi(x_i, y_j) - \sum k_{st}\varphi(u_s, v_t) = 0,$$

$$\sum l_{ij}\varphi(x_i, y_j) = \sum k_{st}\varphi(u_s, v_t).$$

这说明 f^* 为一确定映射.

由于 f^* 是“逐点”进行的，易证它是模同态.

设 $(x, y) \in M \times N$，则有

$$\begin{aligned}(f^*f)((x, y)) &= f^*f((x, y)) \\ &= f^*(x \otimes y) = \varphi(x, y),\end{aligned}$$

即图形可换.

最后，往证 f^* 的唯一性. 设 f^1 也是 $M \otimes N$ 到 P 的 R 模同态且在 $M \times N$ 上有

$$f^1 f = \varphi = f^* f.$$

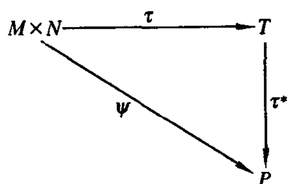
任取 $\sum r_{ij}(x_i \otimes y_j) \in M \otimes N$，则

$$f^*\left[\sum r_{ij}(x_i\otimes y_j)\right]=\sum r_{ij}\varphi(x_i,y_j)$$
$$=\sum r_{ij}f^1f((x_i,y_j))=f^1\left[\sum r_{ij}f((x_i,y_j))\right]$$
$$=f^1\left[\sum r_{ij}(x_i\otimes y_j)\right],$$

即知 $f^*=f^1$.

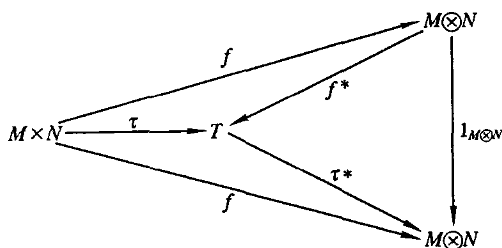
进一步，还有如下的“唯一性”定理.

定理 2　设 R 是个交换环，M 和 N 是 R 模；T 是交换群，且有 $M\times N$ 到 T 的一个平衡映射 τ，对于 $M\times N$ 到任意交换群 P 的平衡映射 Ψ 都有唯一的 T 到 P 的群同态，使图形



可换，则 T 与 $M\otimes_R N$ 群同构.

证明　看图，



对于平衡映射 τ，必有唯一的 $f^*: M\otimes N\to T$ 使 $\tau=f^*f$，而对于平衡映射 f，又必有唯一确定的 $\tau^*: T\to M\otimes N$，使 $f=\tau^*\tau$. 于是得

$$f = \tau^* \tau = (\tau^* f^*) f,$$

但只能有唯一的群同态 $\rho: M \otimes N \to M \otimes N$ 使 $\rho f = f$，ρ 乃是 $M \otimes N$ 上的恒等映射 1，即 $\tau^* f^* = 1$，同理 $f^* \tau^* = 1_T$，这说明 f^* 是 $M \otimes N$ 到 T 的同构映射.

由于这种同构性，今后再提到 M 和 N 的张量积可不考虑其具体由 F 和 G 构造的过程，而只利用定理 1 和定理 2 揭示的"泛性"，所谓 M 和 N 在 R 上的张量积就是 $M \times N$ 到交换群 T 的一个平衡映射 τ，它具有所说的"泛性"，而且我们记 $x \otimes y = \tau(x, y)$.

命题 3 对任意右 R 模 M 都有 $M \otimes_R R \cong M$.

证明 建立映射

$$\varphi: M \times R \to M,$$
$$\varphi: (x, r) \to xr.$$

容易看出这是个平衡映射，利用泛性，必有唯一的群同态 f^* 使下图可换：

$$\begin{array}{ccc} M \times R & \xrightarrow{\otimes} & M \otimes_R R \\ & \searrow^{\varphi} & \downarrow f^* \\ & & M \end{array}$$

注意 f^* 是 R 同态，且 $f^* \otimes = \varphi$，故

$$f^* \left[\sum l_{ij}(x_i \otimes y_j) \right] = \sum l_{ij} \varphi(x_i, r_i) = \sum l_{ij} x_i r_j.$$

对于任意 $x \in M$，$f^*(x \otimes 1) = x1 = x$，即知 f^* 是个满射.

如果有 $a = \sum l_{ij}(x_i \otimes r_j) \in M \otimes R$ 使 $f(a) = 0$，即 $\sum l_{ij} x_i r_j = 0$，那么，由 $x_i \otimes r_j = x_i r_j \otimes 1$ 可知

$$a = \left(\sum l_{ij} r_j x_i \right) \otimes 1 = 0 \otimes 1 = 0,$$

f^* 为单射.

所以，f^* 是 $M \otimes R$ 到 R 的同构映射.

命题 4 对任意 R 模 M、N 都有 $M \otimes_R N \cong M \otimes_R M$.

证明 建立 $M \times N$ 到 $N \otimes M$ 的映射 φ，

$$\varphi: (x, y) \to y \otimes x, \quad x \in M, y \in N,$$

显然 φ 是平衡映射. 利用 $M \otimes_R N$ 的泛性，必有 $M \otimes N$ 到 $N \otimes M$ 的群同态 f^* 使 $\varphi = f^* \otimes$. 于是，对任意 $(x, y) \in M \times N$，有

$$f^*(x \otimes y) = (f^* \otimes)((x, y)) = \varphi(x, y) = y \otimes x.$$

同理，有 $N \otimes M$ 到 $M \otimes N$ 的群同态 g^*，使

$$g^*(y \otimes x) = x \otimes y.$$

进一步，易知 $f^* g^* = 1$，$g^* f^* = 1$，从而知 f^* 为同构映射.

命题 5 若

$$f: M \to M', \qquad g: N \to N'$$

均为 R 模同态，则必有唯一确定的 $M \otimes_R N$ 到 $M' \otimes_R N'$ 的群同态映射 σ，使得

$$\sigma(x \otimes y) = f(x) \otimes g(y).$$

证明 看 $M \times N$ 到 $M' \otimes N'$ 的映射 φ，

$$\varphi(x, y) = f(x) \otimes g(y),$$

易知 φ 是个平衡映射. 利用 $M \otimes N$ 的泛性，必有 $M \otimes N$ 到 $M' \otimes N'$ 的唯一确定的群同态 σ，使下图可换：

$$\begin{array}{ccc} M \times N & \xrightarrow{\otimes} & M \otimes N \\ & \searrow^{\varphi} & \downarrow \sigma \\ & & M' \otimes N' \end{array}$$

即对任意 $x\in M$，$y\in N$ 有

$$\begin{aligned}\sigma(x\otimes y) &= (\sigma\otimes)((x,y))\\ &= \varphi(x,y)=f(x)\otimes g(y).\end{aligned}$$

由于映射 σ 是由 f，g 唯一确定的，就把 σ 记为 $f\otimes g$，即有

$$(f\otimes g)=(x\otimes y)=f(x)\otimes g(y),\quad x\in M,\ y\in N.$$

当然，对 $M\otimes N$ 的任意元 $\sum r_{ij}(x_i\otimes y_j)$ 有

$$(f\otimes g)\left[\sum r_{ij}(x_i\otimes y_j)\right]=\sum r_{ij}f(x_i)\otimes g(y_j).\quad (*)$$

这里，我们是利用泛性导出 $f\otimes g$ 的定义，而不是把(*)当成定义式，表面绕开了合理性问题.

对于一般非交换环上的左、右模的张量积理论的研究也很重要，但需要更多的准备知识，不在本课中介绍了.

名词索引

（拼音序）

[General Information]
书名=近世代数基础
作者=牛风文编
页数=194
SS号=11160961
DX号=
出版日期=2002年08月第1版
出版社=吉林大学出版社